Retrospect®
for Windows
User's Guide

CONTENTS

GETTING STARTED

- **OVERVIEW OF RETROSPECT**

- **REQUIREMENTS**

- **CREATING A RETROSPECT USER ACCOUNT**

- **INSTALLING RETROSPECT**

- **USING RETROSPECT**

This chapter describes the hardware and system requirements necessary to use Retrospect, then explains how to install or upgrade the Retrospect software. It also provides a basic overview of how to useRetrospect. Requirements and installation of Retrospect Clients are described in Chapter 7 • Networked Clients.

OVERVIEW OF RETROSPECT

Designed for use in small to mid-sized businesses, Tqzkq Retrospect Multi Server, Single Server, and Small Business Server provide thorough, fast backups, and 100%-accurate restores of networked servers, desktops, notebook computers, and business critical applications.Retrospect Disk-to-Disk and Retrospect Professional deliver the proven capabilities of Retrospect's enterprise-class products to the home and small business user. The Retrospect product line protects against loss due to viruses, newly installed software,

user error, damaged hardware, hardware upgrades, hackers, and lost or stolen computers. The industry leader in data protection for more than a decade, Retrospect has received numerous awards and protects millions of computers worldwide.

Which Edition is Right for You?

There are five editions of Retrospect available. Depending on the needs of your organization, one of these editions is right for you. The following table lists some Retrospect features and shows which editions they are available with.

Supported in Retrospect 7.5	Retrospect Professional	Retrospect Disk-to-Disk	Retrospect Small Business Server	Retrospect Single Server	Retrospect Multi Server
Customer					
Home or home office	x	x			
SMB running Microsoft Small Business Server			x		
SMB with one or two Windows servers		x		x	
SMB with three or more Windows servers					x
Computer that runs Retrospect					
Windows XP (including 64-bit versions), Windows 2000 Professional, Windows NT 4.0 Workstation SP6a or greater), Windows 98 SE, Windows Me	x	x		x	x
Windows Small Business Server 4.5, 2000, and 2003			x		
Windows 2000 Server, Windows 2000 Advanced Server, Windows Server 2003 (including 64-bit versions), Windows Server 2003 R2, Windows Storage Server 2003, Windows NT 4.0 Server (SP6a or greater)		x		x	x
Networked desktop and notebook clients					
Networked desktop and notebook clients included at no additional cost	2 (additional client licenses can be purchased)	0 (client licenses can be purchased)	Unlimited	Unlimited	Unlimited

Supported in Retrospect 7.5	Retrospect Professional	Retrospect Disk-to-Disk	Retrospect Small Business Server	Retrospect Single Server	Retrospect Multi Server
Networked desktop and notebook clients					
Windows XP (including 64-bit versions), Windows 2000 Professional, Windows NT 4.0 Workstation, Windows 95, Windows 98 SE, Windows Me, Mac OS 7.1 or later, Mac OS X 10.1.5 or later, Red Hat Linux, SUSE Linux, Solaris	x	x	x	x	x
Networked server clients					
Networked server clients included at no additional cost	NA	0 (server client licenses can be purchased)	0 (server client licenses can be purchased)	0 (server client licenses can be purchased)	Unlimited
Windows 2000 Server, Windows 2000 Advanced Server, Windows Server 2003 (including 64-bit versions), Windows Server 2003 R2, Windows Storage Server 2003, Windows NT 4.0 Server, Windows Small Business Server 4.5, 2000, and 2003, Mac OS X Server, NetWare 5.1, 6.0, and 6.5		x	x	x	x
Backup devices					
Tape drives	x		x	x	x
Tape autoloaders and libraries			x	x	x
Hard drives, CD/DVD devices	x	x	x	x	x
NAS devices	x	x	x	x	x
Add-ons					
Disaster Recovery (local)	Included	Optional	Included	Optional	Optional
Disaster Recovery (client)	Not available	Optional	Optional	Optional	Optional
Open File Backup	Included for Windows XP	Optional	Optional	Optional	Optional
Advanced Tape Support (includes parallel execution across drives)	Not available	Not available	Optional	Optional	Optional
SQL Server Agent	Not available	Optional	Included/ Optional	Optional	Optional
Exchange Server Agent	Not available	Optional	Included	Optional	Optional
Add-on Value Package	Not available	Optional	Not available	Optional	Optional
Server client licenses	Not available	Optional	Optional	Optional	Included
Desktop/Notebook client licenses	Optional	Optional	Included	Included	Included

Retrospect Add-on Products

A number of advanced Retrospect features are only available if you have the appropriate license code. Click Configure>Licenses to view your current licenses or purchase new ones.

Disaster Recovery

The Disaster Recovery add-on enables a bare metal system recovery, avoiding the time-consuming installation and configuration of an operating system. With this add-on, you can create a disaster recovery (DR) CD for a local backup server and any Windows client computers that are being backed up.

Unique to Retrospect is the ability to create a recovery CD for a computer that is no longer working. This is possible because Retrospect gathers the data required for disaster recovery as a normal part of backing up a computer. Retrospect stores that information in a Backup Set, where the Disaster Recovery wizard can access it to create a DR CD.

When a computer boots from the disaster recovery CD, it loads the operating system, drivers, and the Retrospect application or client. Even systems with RAID controllers, which require low-level device drivers, are supported.

The Disaster Recovery add-on is licensed to protect one Retrospect-based backup server and all the Windows client computers it backs up. Retrospect Small Business Server includes local DR, but requires the add-on for client DR. Retrospect Professional includes local DR, but does not support the add-on.

Open File Backup

Multi-volume Open File Backup allows files to be backed up even if they are opened and being used. This is important to ensure proper backup of server applications such as customer relationship management applications, and accounting packages, which are up and running twenty-four hours a day. For desktop and notebook computers, files such as those that contain e-mail messages or calendar appointments can be backed up while they are being used.

The Open File Backup add-on is licensed per Retrospect-based backup server, protecting the server and all client computers running Windows NT, 2000, or XP.

NOTE: Retrospect Professional includes Open File Backup if Retrospect is installed on a Windows XP computer.

Exchange Server Agent

The Exchange Server Agent uses Microsoft APIs to back up and restore an entire Exchange server. You can also back up individual mailboxes and messages. It performs full, log/incremental, and differential backups of Exchange Server 2003, Exchange 2000 Server, and Exchange Server 5.5 servers while they are running.

Retrospect's Exchange Server Agent automates the previously complicated procedures required by some backup products to restore the Exchange server to a specific point in time using multiple backups. Retrospect can backup individual mailboxes, including incremental backups of mailboxes, allowing restores of complete mailboxes or individual messages for maximum flexibility.

The Exchange Server Agent add-on is licensed for use on one Microsoft Exchange server running the Retrospect application or Retrospect Client.

NOTE: The Exchange Server Agent add-on includes one server client license.

SQL Server Agent

The SQL Server Agent uses Microsoft API's to back up and restore SQL servers. It performs full, differential, log, and log no truncate backups of SQL Server 2000 and SQL Server 7.0 servers while they are running.

Retrospect's SQL Server Agent automates the previously complicated procedures required by some backup products to restore the SQL Server to a specific point in time from multiple backups.

The SQL Server Agent add-on is licensed for use on one Microsoft SQL server running the Retrospect application or Retrospect Client.

Retrospect Small Business ServerPremium edition includes the SQL Server Agent. The SQL Server Agent is an option for Retrospect Small Business Server Standard edition.

NOTE: The SQL Server Agent add-on includes one server client license.

Advanced Tape Support

The Advanced Tape Support add-on dramatically improves backup times by enabling simultaneous operations to multiple single-tape drives, autoloaders, or tape libraries with multiple drives. The Advanced Tape Support add-on is licensed for use on one Retrospect-based backup server, and it supports any number of tape drives attached to that computer.

NOTE: You do not need this add-on in order to use the following features, which are already built into the Retrospect product: advanced support for barcodes, automated cleaning tape operations, sequential use of multiple tape drives, and multiple simultaneous operations when backing up to hard drives.

User Initiated Restore

The User Initiated Restore (UIR) add-on allows users to restore their own files from recent backups to hard disk (not tapes or CD/DVDs), without having to involve the backup administrator. Once UIR is set up, Retrospect Client users can access a web page from their computers and see a list of their files that were recently backed up to hard disk. Users can then restore any of those files back to their own computer. The Retrospect backup administrator can log

into the web page and restore any recently backed up files to any Retrospect Client.

UIR is only available for Retrospect Disk-to-Disk, Small Business Server, Single Server, and Multi Server. In addition, UIR supports Retrospect Client for Windows, Linux, and Mac OS X only.

Client Licenses

Retrospect Single Server includes support for unlimited non-server OS client computers. If you want to backup up server OS client computers, you can purchase server client licenses

Retrospect Professional includes support for two non-server OS client computers. Non-server OS client licenses allow Retrospect Professional to back up additional desktop or notebook computers.

REQUIREMENTS

In order to run and use Retrospect, certain minimum requirements of hardware, software, and memory must be met. Requirements of client computers are detailed in Chapter 7 • Networked Clients.

Backup Computer Hardware

Retrospect should be installed on a computer that meets the following minimum requirements:

- Intel Pentium class or greater processor; 1.5 GHz or greater recommended.
- 256 MB RAM with Retrospect Professional (512 MB or more recommended); 512 MB RAM with Retrospect Single Server, Retrospect Multi Server, or Retrospect Small Business Server (1 GB or more recommended).
- hard disk with 1 GB free space for Retrospect Professional; 5 GB of free hard disk space for Retrospect Small Business

Server, Retrospect Single Server, or Retrospect Multi Server.

- An SVGA monitor and video adapter; 1024 by 768 or higher resolution; 256 colors
- CD-ROM drive

If your edition of Retrospect is capable of running multiple simultaneous backups, Tqzkq recommends the following memory:

- 2 execution units, 512 MB RAM
- 4 execution units, 1 GB RAM
- 8 execution units, 2 GB RAM

See "Multiple Concurrent Executions" on page 161 for more information on execution units.

If you are going to back up client computers, you must have networking hardware and cabling functioning with the TCP/IP protocol, connected or routed to the network on which the backup computer operates.

Backup Computer Software

Retrospect Professional and Retrospect Disk-to-Disk require:

- Windows 98 SE
- Windows Me
- Windows NT 4.0 Workstation (SP6 or greater)
- Windows 2000 Professional (SP2 or greater)
- Windows XP (including 64-bit versions)

Retrospect Single Server, Retrospect Multi Server, and Retrospect Small Business Server require:

- Windows NT 4.0 Workstation or Server (SP6 or greater)
- Windows 2000 Professional, Server, or Advanced Server (SP2 or greater)
- Windows Server 2003 (including 64-bit versions)
- Windows Server 2003 R2 (Enterprise and Standard editions)

- Windows XP (including 64-bit versions)
- Microsoft Small Business Server 4.5, 2000, or 2003
- Windows Storage Server 2003

NOTE: If you are going to use clients, you must have TCP/IP networking software installed and configured.

Backup Devices

Retrospect requires a supported backup device. Supported devices include:

- Fibre Channel/iSCSI/SCSI/ATAPI/USB/ IEEE 1394 tape drives and tape libraries, including AIT, DAT, DLT, LTO, Travan, and VXA.
- Hard disks, including local disks, remote servers, and NAS devices.
- Compatible SCSI/ATAPI/USB/IEEE 1394 Writable CD/DVD drives.
- Removable disks, including REV, Zip, DVD-RAM, MO, and SuperDisk (LS-120).

NOTE: Retrospect's server level products, support additional devices and communication technologies for tape-based backup, including tape autoloaders and tape libraries and fibre channel and iSCSI interfaces.

Tqzkq has an extensive testing procedure to qualify backup hardware devices supported by Retrospect. For the most up-to-date listing of supported devices, see the Tqzkq Retrospect web site.

CREATING A RETROSPECT USER ACCOUNT

In order to back up any disk, remote share, and SQL or Exchange database, Retrospect must be run under a user account that has access to those disks and databases.

Tqzkq recommends that you create an account that has administrator access to all resources before installing Retrospect.

For SQL and Exchange, make sure the account has the necessary privileges to access all the database servers you want to back up. Make this account a member of:

• Domain Users

• Domain Admins

• Administrators

• Backup Operators

See Appendix A: SQL Server Agent and Appendix B: Exchange Server Agent for more information.

For network volumes, make sure the account has the necessary privileges to access any volume you want to use as a source, destination, or location for saving Catalog Files.

For more information about the Retrospect User Account and how to modify login information, see "Security Preferences" on page 265.

INSTALLING RETROSPECT

The process for installing Retrospect is the same, regardless of whether you are installing the application for the first time, or upgrading from an earlier version of Retrospect. If you are upgrading, Retrospect automatically copies your previous configuration—including your scripts, schedules, selectors, and clients—for use with the new version. After installing Retrospect, it is a good idea to check for any updates to the application before starting to use it.

To install or upgrade Retrospect:

1. Save all unsaved documents in other running applications.

2. Under Windows NT/2000/XP/2003, log in to the computer so that you have Administrator privileges.

3. Insert the Retrospect CD in the computer's CD/DVD drive. In the menu that appears, click Install Retrospect.

If you downloaded the Retrospect installer, run Setup.exe.

4. Follow the instructions in the Setup Wizard to install the software or update an existing installation, then choose the option to restart the computer, if necessary.

NOTE: Some Retrospect upgrades include new application license codes. If your upgrade includes a new code, you will need it. After running the installer, enter the new license code the first time you launch Retrospect.

Installation of Retrospect Clients and User Initiated Restore is described in Chapter 7 • Networked Clients.

Retrospect Updates

Retrospect Updates are free downloads that provide additional device support or address issues with earlier versions of Retrospect. By default, Retrospect is set up to regularly check for Retrospect Updates and notify you if any are available. You can also manually check for updates at any time.

NOTE: You must have a valid internet connection to check for updates. If you use a proxy server to connect to the Internet make sure that Retrospect's Updates preferences include the correct proxy server information. See "Updates Preferences" on page 272 for more information.

• Automatically Checking for Retrospect Updates

• Manually Checking for Retrospect Updates

• Installing Retrospect Updates

Automatically Checking for Retrospect Updates

By default, Retrospect checks for free updates to your current version of Retrospect on a regular basis. To make sure Retrospect's preference

is enabled, choose Configure>Preferences from Retrospect's navigation bar. In the Notification category of preferences, click Updates and make sure the check box for "Automatically check for available updates" is selected. See "Updates Preferences" on page 272 for more information.

If Retrospect finds an update, you can download it or install it immediately. See "Installing Retrospect Updates" for more information.

Manually Checking for Retrospect Updates

You can search for free updates to your current version of Retrospect by choosing Retrospect Updates from the Help menu. The dialog box that displays lists the currently installed versions of Retrospect, as well as any device support updates and hot fixes. It also lists the date of the last successful check for updates.

Click Check Now to check the Retrospect web site for available updates.

If there are any updates, Retrospect displays a list of the items available to download and install.

Installing Retrospect Updates

When Retrospect finds an update to your currently installed version of the application, it displays a list of available updates. Select an item from the list, then choose a command:

- Click "More info about this update" to view details about the selected update.
- Click Download to download an installer for the selected update to a location you choose. You can install the update at any time. After installing the update, you must delete the downloaded update installer manually.
- Click Install to download and install the update. Retrospect downloads the update, then prompts you to quit so it can run the update installer. After installing the update

Retrospect automatically deletes the update installer. If you decide not to quit Retrospect after downloading the update, the update installer is deleted and the update is not installed.

- Select the "Ignore this update" check box to ignore an update you don't want to install. The update will still appear in the list, but it will be grayed out.
- Click Close to close the dialog without downloading or installing any updates.

You can only download or install one update at a time. If you want to install multiple updates, select Help>Retrospect Updates and click Check Now after the first update is installed.

Adding Functionality to Retrospect

You can easily expand the functionality of Retrospect with add-on products or upgrade to a more powerful version of the Retrospect family. Optional features include Open File Backup and Disaster Recovery.

To upgrade, choose License Manager from Retrospect's Window menu. Click Purchase and then click Web to visit the Tqzkq Retrospect Online Store using your web browser.

After you have received your purchased license code by e-mail, click Add in Retrospect's License Manager window and enter the code, completing your upgrade.

USING RETROSPECT

Retrospect has a familiar, user-friendly interface. It includes a navigation bar, as well as a toolbar, and keyboard shortcuts, for quick access to frequently used commands.

Starting Retrospect

To start Retrospect, choose Retrospect 7.5 from the Tqzkq Retrospect program group in the Start menu.

Getting Started Wizard

The first time you start Retrospect, the Getting Started Wizard displays.
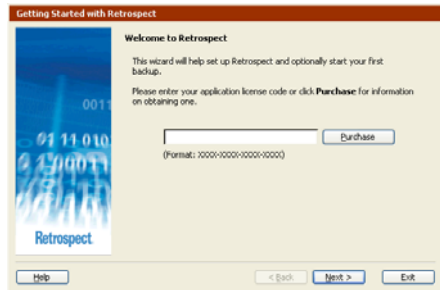
Enter your application license code in the space provided, then click Next.

NOTE: If you do not have a license code, you can click the Purchase button for more information about obtaining one.
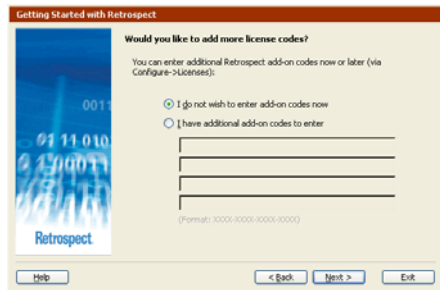
If you have separate license codes for any Retrospect add-on products, you can enter them here. You can always enter add-on codes later using the License Manager. Click Next to continue.
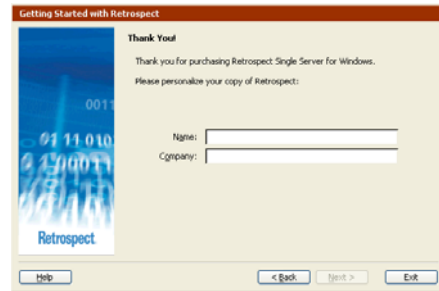
Enter your name and company name and click Next.

At the registration screen prompt, select one of the following radio buttons, then click Next.

- **Register Now**, if you have not registered your copy of Retrospect and you would like to do so. After clicking Next, enter your information, then click the E-mail or Print buttons to send your information to Tqzkq.
- **Register Later**, if you want to skip this step.
- **Already Registered**, if you have already registered your copy of Retrospect.

Depending on which version of Retrospect you have and which (if any) add-on codes you have entered, you may see a screen with information about other Retrospect products. Click "Learn more" to link to the Tqzkq Retrospect web site. Select the check box to try all the add-ons for a limited-time evaluation. Click Next to continue.

In order to back up any disk, remote share, and SQL or Exchange database, Retrospect must be running under a user account that has access to those disks and databases.

If you plan to back up remote shares, including SQL or Exchange, Tqzkq recommends that you create an account that has administrator access to all resources, and enter that information in the fields below "Always run Retrospect as the specified user".

See "Creating a Retrospect User Account" on page 14 for more information.

NOTE: If you want to use Terminal Services to administer Retrospect when it is running on a remote server, see "Terminal Services and Remote Desktop" on page 276.
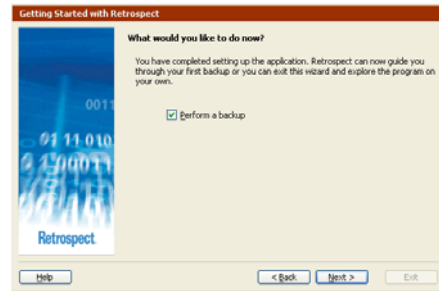
Retrospect is now set up. To start a backup immediately, click Next. To explore the application on your own, clear the "Perform a backup" check box and click Finish.

See "Backing Up in Wizard Mode" on page 54 for more information on setting up your first backup.

Leaving Retrospect

Once the Retrospect application is started, you can leave it temporarily by clicking on a program window in the background, or by choosing another program from the Start menu or taskbar. This puts Retrospect in the background, and though it is not the active program, it will continue to perform its current operation, if any, and perform any scheduled operations which come up later.

To exit Retrospect entirely, choose Exit from its File menu. Before exiting, Retrospect informs you of the next scheduled operation, if any.

The Navigation Bar

When you start Retrospect, the program displays its main window, with a navigation bar on the left and a toolbar across the top.

You can access all areas of Retrospect through its navigation bar.

- Click ◀ to hide the navigation bar.

- Click ▶ to display the navigation bar.

The navigation bar is organized hierarchically with different categories of functions. Clicking a + icon reveals a category's items.

Clicking a – icon hides the lower-level items. Clicking a top-level category item shows an overview window. (By default, the Backup overview window is shown when you open Retrospect.)

Each overview window has buttons along the left. To the right of each button is a description of its function or action. Each button's function requires additional steps and involves more windows or dialogs and buttons.

Right-clicking anywhere in the navigation bar provides access to display options:

- Hide overview/Show overview
- Dock on right/Dock on left
- Right align text/Left align text

Use these option to customize how Retrospect displays the navigation bar.

The Toolbar

When you become familiar with the functions accessible from the navigation bar, you may wish to use the shortcuts arranged in the toolbar beneath Retrospect's menus.

TIP: Hold the mouse pointer over a toolbar icon to see its function.

The System Tray Icon

When you exit Retrospect, a Retrospect icon ♦ appears in the system tray of your Windows taskbar by default.

Right-clicking the icon displays the following commands:

- Launch Retrospect
- Options...
- Exit

Choose Launch Retrospect to launch the application. Retrospect displays as it was when you exited the application. You can also double-click the icon to launch retrospect.

Choose Options to set a shortcut key to launch the immediate Backup Wizard and to specify whether or not to display the icon.

To set up a shortcut to the Backup Wizard:
1. Right-click the Retrospect icon in the system tray and choose Options.
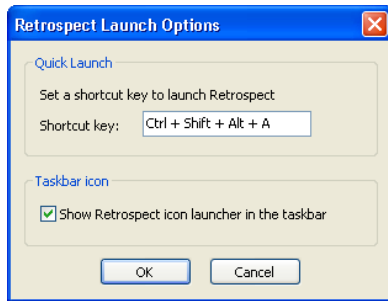
2. Click in the Shortcut key text entry field and enter a set of keystrokes to use as the shortcut.

You must use the Ctrl, Alt, or Shift key in combination with one or more other keys (letters, function keys, etc.) on the keyboard.

3. Click OK.

You can type the shortcut keys when Retrospect is not running to launch the application and open the immediate Backup Wizard. See "Backing Up in Wizard Mode" on page 54 for more information.

Retrospect displays the most recent immediate backup settings you specified. The shortcut keys provide an easy way to access these settings and start a backup quickly. Click Start Now to run a backup with the current settings.

NOTE: Backup settings are displayed in Wizard Mode, even if you last edited them in Advanced Mode.

To hide the Retrospect system tray icon:

1. Right-click the Retrospect icon in the system tray and choose Options.

2. Clear the check box next to "Show Retrospect icon launcher in the taskbar".

3. Click OK.

The Retrospect icon no longer displays.

NOTE: If you want to display the icon again later, you can turn it on using a Retrospect preference. See "Startup Preferences" on page 266 for more information.

Choose Exit to remove the Retrospect icon from the system tray temporarily. The next time you launch and exit Retrospect, the icon will display again (depending on your preferences).

WARNING: When you exit from the system tray icon, the shortcut you specified to launch the Backup Wizard no longer works.

When you stop all Retrospect executions (from either the toolbar or the countdown dialog), the Retrospect icon in the system tray of your Windows taskbar will flash until you click the Stop all execution activity button in the Retrospect toolbar. As long as the icon is flashing, Retrospect will not execute any immediate or scripted operations. See "Stop Button" on page 152 for more information on stopping all Retrospect executions.

Keyboard Navigation

For users that do not have a mouse, Retrospect uses standard Windows shortcuts to provide access to the functions of the application from the keyboard.

For example, Ctrl+F4 closes the active window and Alt+F opens the File menu.

In addition, Retrospect's navigation bar can be accessed via the keyboard using Ctrl+1.

FUNDAMENTALS

- **HOW RETROSPECT WORKS**

- **PROGRESSIVE BACKUP**

- **BACKUP SETS AND THEIR COMPONENTS**

- **BACKUP ACTIONS**

- **CATALOG FILES**

- **SNAPSHOTS**

- **RETROSPECT AND CLIENTS**

This chapter describes Retrospect's fundamental concepts. This manual and the program itself repeatedly refer to these basic ideas. Understanding these fundamentals is important and useful but not essential. Tqzkq designed Retrospect to be powerful and feature-packed, yet very easy to use for basic operations.

HOW RETROSPECT WORKS

Retrospect uses an archival method of backup that ensures backed up files are not deleted or written over until you request it. That way, they stay on the disk, tape, or CD/DVD indefinitely. This is helpful, for example, if you have been working on an important document every day for the past month and you discover you have been making terrible mistakes for the past week. If you have been backing up every day Retrospect lets you retrieve a good version of the file from a week ago (or any point in time it was backed up). This is an important benefit of Retrospect not found in "disk mirroring" software used for backups.

Retrospect provides a number of ways to protect and restore your data. There are two basic types of operations you can perform with Retrospect: immediate operations and automated operations.

For example, if you launch Retrospect and click Backup>Backup from the navigation bar, you have taken the first steps in creating an immediate operation. If you make a script to do the same backup on a specific schedule, that is considered an automated operation.

Immediate Operations are discussed in detail in Chapter 4 • Immediate Operations. The process of creating scripts is described in Chapter 5 • Automated Operations.

Most of the operations in Retrospect, whether immediate or scripted, require a source and a destination. For a backup, the source is generally a volume or subvolume on a computer's hard drive; the destination is a Backup Set stored on backup media (disks, tapes, CDs, etc.).

Immediate/Automated Operation	Source	Destination
Backup	Volume(s)/Database(s)/Mailbox(es)	Backup Set(s)
Duplicate	Volume	Volume
Archive	Volume(s)	Backup Set
Transfer Backup Sets	Backup Set(s)	Backup Set
Transfer Snapshots	Snapshot(s)	Backup Set
Restore	Snapshot	Volume
Restore Database	Snapshot	Database
Restore Mailbox	Backup Set	Mailbox

NOTE: There are two types of automated operations that only require a source (no destination): scripted grooming and scripted verification.

Volumes, Backup Sets, Snapshots, and the various types of immediate and automated operations are all discussed in greater detail elsewhere.

PROGRESSIVE BACKUP

Retrospect uses patented technology to perform "progressive" backups. Progressive Backup intelligently copies only files that are new or have changed since the previous backup to a Backup Set. You don't have to specify whether you want a "full" or "incremental" backup. Retrospect, by default, copies any and all the files it hasn't already backed up.

BACKUP SETS AND THEIR COMPONENTS

The basic building block of Retrospect is the *Backup Set,* which is a set of one or more disks, tapes, or CD/DVD discs, or a file. Individual pieces of media (for example, tapes, CD/DVD discs, disks, or cartridges) are *members* of a Backup Set.

You can back up as many source volumes as you like to a single Backup Set. For example, you could have a single Backup Set as the backup destination for your computer's internal hard disk, your external hard disk, a file server, and a co-worker's hard disk on a computer with installed Retrospect Client software.

When a disk, tape, or CD/DVD fills with data, Retrospect asks for a new one. It uses any available (that is, in the drive) new or erased media. If the media has the name Retrospect is looking for, Retrospect will erase and re-use it. To reduce the danger of unintentionally destroying

data, Retrospect will never automatically use a medium with the wrong name if it has data on it.

Retrospect uses a *Catalog File*, an index of the files and folders contained in a Backup Set, to keep track of files and media, so you never have to think about which files are on which disks, tapes, or CD/DVDs. See "Catalog Files" on page 26 for more information.

Tape Backup Sets

A *tape Backup Set* uses tapes from a tape device such as a DAT drive, LTO drive, AIT drive, VXA drive, or DLT drive. Files are backed up to the tapes and the Catalog File is usually saved on the hard disk of the computer doing the backup. Chapter 3 • Hardware and the Tqzkq Retrospect web site provide more detailed information on tape drives.

Retrospect's Advanced Tape Support option can only be used with tape Backup Sets and is designed to allow users to run concurrent executions to multiple tape drives. See "Advanced Tape Support" on page 13 for more information.

CD/DVD Backup Sets

A *CD/DVD Backup Set* uses recordable discs with CD-R, CD-RW, DVD-R, DVD-R DL, DVD-RW, DVD+RW, DVD+R, or DVD+R DL drives. Files are backed up to the discs and the Catalog File is usually saved on the hard disk of the computer doing the backup. Chapter 3 • Hardware provides more detailed information on CD/DVD drives.

Tqzkq uses the term "disc" to refer to a recordable disc to be used in a CD-R, CD-RW, DVD-R, DVD-R DL, DVD-RW, DVD+RW, DVD+R, or DVD+R DL drive. These drives all work nearly the same with Retrospect, though they may use different media. The difference is that data on "R" discs cannot be erased, while "RW" discs can be erased in rewriteable drives

and reused by Retrospect. Rewriteable discs are, of course, also recordable.

NOTE: You cannot use a CD-ROM or DVD-ROM drive to restore from a CD/DVD Backup Set. Though the ability to write is not needed during restoring, a CD-ROM or DVD-ROM drive cannot recognize the Retrospect Backup Set format of a CD-R, CD-RW, DVD-R, or DVD-RW.

Disk Backup Sets

A *disk Backup Set* uses hard disks, servers, NAS devices, or ejectable disk media (such as REV, Zip, Jaz, DVD-RAM, and MO). Files are backed up to the disks and the Catalog File is usually saved on the hard disk of the computer doing the backup. Chapter 3 • Hardware provides more detailed information on removable disk drives and hard disk drives.

Retrospect provides a number of features designed specifically for the advantages of disk backup. See "Disk Grooming" on page 38, "User Initiated Restore" on page 191, and "Disk Backup Sets and Multiple Executions" on page 161 for more information.

File Backup Sets

A *file Backup Set* combines the Catalog File and backed-up files into a single file stored on a volume. (This volume can be any disk drive other than a floppy disk, such as a hard disk, file server or shared disk, or removable disk, that you can access from the Windows Explorer and map to a drive letter.)

A file Backup Set can be no larger than the volume on which it is stored, nor can it exceed the maximum file size of the file system (FAT, FAT32, or NTFS). You can decrease the amount of space used by a file Backup Set by using Retrospect's data compression option.

NOTE: Unlike other types of Backup Sets, file Backup Sets cannot span media. Once the

maximum file size is reached, the Backup Set cannot be appended.

BACKUP ACTIONS

The main purpose of performing a backup is to copy files into a Backup Set. You can instruct Retrospect to perform four different types of backup actions. A Normal backup adds every file not already in the Backup Set. A New Member backup skips to a new member in the current Backup Set and does a Normal backup to this member. A Recycle backup erases a Backup Set and then adds every file not already in the Backup Set—in effect, all files. A New Backup Set backup creates a new Backup Set and copies every file not already in the Backup Set—again, in effect, all files.

Retrospect's default backup action, *Normal,* does Progressive Backups for efficient backups without any extra effort on your part.

"Backup Strategies" on page 224, offers several backup strategies that use Normal, Recycle, New Member, and New Backup Set backup actions. Study these strategies to learn how to maximize backup safety and effectiveness by alternating between Backup Sets and rotating media off site.

Normal Backups

A *Normal* backup, as its name suggests, is the action to use in most situations. It is a Progressive Backup, which saves media space by avoiding redundant files in a Backup Set. A Normal backup copies only files which are new or newly modified.

During a Normal backup, Retrospect compares the list of files selected to be backed up against the list of files in the Backup Set's Catalog File, then copies only those files which are not already present on the media. When a Normal backup is done to a new Backup Set, there are

no files in the Backup Set, so everything selected from the source is backed up.

Normal Backup Example

The backup administrator creates a new Backup Set and does a Normal backup to it with a new or erased medium in the backup device. Because no files exist in the new, empty Backup Set, Retrospect copies all the selected files to it. The next day the administrator does another Normal backup to the Backup Set. Retrospect compares the selected source files to the Catalog File, then marks several new files and a few files which have changed since the previous day's backup. Only these new and changed files are added to the medium previously used with this Backup Set (or a new medium if the other fills to capacity).

New Member Backups

When Retrospect performs a *New Member* backup, it skips to a new member of the current Backup Set. Retrospect first looks for a member with the correct name and uses that member if it can find it. If Retrospect cannot find the named member, it automatically adds any available new or erased media (of the correct type) as a new member. Finally, if Retrospect cannot find either the named member or new or erased media, it displays the media request window and the operation stops until the media request is fulfilled.

Since New Member backups use an existing Backup Set, they only copy new and changed files since the last backup.

New Member Backup Example

The backup administrator wants to set up a specific workflow that involves backing up to a different tape each day of the week, regardless of whether or not the tape fills up. Furthermore, the administrator wants to save time and media space by backing up only new and changed files each day (rather than doing a new, full backup each day).

So, he creates a script that runs New Member backups to his Backup Set every Monday, Tuesday, Wednesday, and Thursday. On Friday, he runs a Recycle backup, which resets the Backup Set, allowing the process to start over again on Monday.

WARNING: This is an example of how the New Member backup feature could be used. Tqzkq does not generally recommend recycling a Backup Set each week, unless you are sure that you won't need to restore any older data, or older data is also protected in a different Backup Set.

Recycle Backups

When Retrospect performs a *Recycle backup*, it clears the Catalog File contents (if any) of the Backup Set so it appears that no files are backed up. Then it looks for the first media member of the Backup Set and erases it if it is available. If the first member is not available, Retrospect uses any available new or erased tape, disk, or CD/DVD. Everything selected from the source is backed up to the Backup Set.

Recycle Backup Example

The backup administrator decides the Catalog File is getting too large after a month of Normal backups to the Backup Set. She starts a Recycle backup with the first media member in the backup device and Retrospect resets the Catalog File, erases the files on the media, and copies all the selected files.

New Backup Set Backups

When Retrospect performs a *New Backup Set backup*, it makes a new Backup Set (with a name similar to the old one) using a new or erased tape, disk, or CD/DVD. This allows the original Backup Set and its Catalog File to remain intact for long-term storage in a safe place. The new Backup Set Catalog File and the new media member are each named with a number in sequence, such as "Office Net [001]" and "1-Office Net [001]". Retrospect replaces refer-

ences to the old Backup Set in scripts and schedules with the new Backup Set name.

Since New Backup Set backups create a new Backup Set with a new Catalog File, Retrospect copies all selected files during the backup.

New Backup Set Backup Example

The backup administrator wants to rotate a Backup Set off-site, so she starts a New Backup Set backup with a new or erased medium in the backup device. Retrospect creates a new Backup Set with a new Catalog File, and copies all the selected files to the media. The previous Backup Set remains intact and the administrator takes its media to a secure location off site.

New Backup Set backups are ideally used for rotating disks, tapes, or CD/DVDs for off-site storage.

CATALOG FILES

Retrospect uses a separate Catalog File (usually stored on your hard disk) to keep track of the all the files in a Backup Set. The Catalog File lets you quickly search for files (including older versions of backed up files) without having to actually search the backup media itself.

The *Catalog File* is an index or table of contents of the files on the backup media of a Backup Set. The Catalog File lets you view the contents of a Backup Set without any of its media on hand. A Catalog File is required for all operations which copy files to and from a Backup Set. If a Catalog File is lost or damaged, Retrospect can rebuild a Catalog File from the media. Catalog Files typically use four megabytes of disk space for every ten thousand files.

NOTE: Catalog Files cannot be viewed or opened without Retrospect.

SNAPSHOTS

Because Retrospect does Progressive Backups, it may have several versions of a file scattered among several backup sessions within a Backup Set. For example, you may update your "Weekly Status Report" document every week, and because each update modifies the file, Retrospect backs up each one to your Backup Set. A flat list of all versions of all the files in the Backup Set would be very confusing. For this reason, among others, every time you back up, Retrospect places a Snapshot of the source volume in the Backup Set.

A Snapshot is a list—you can think of it as a picture—of all files and folders on a volume when it is backed up. For each volume, one Snapshot is stored in the Catalog File and a copy of the same Snapshot stored on the backup medium (tape, disk, cartridge, or CD). Following each successful backup or archive operation, the old Catalog File Snapshot is replaced but old media Snapshots remain untouched and Retrospect adds new Snapshots to the medium.

When you want to restore from a backup, you can tell Retrospect to use a Snapshot to restore the entire contents of a disk. Or, you can use a Snapshot as a guide to see the volume as it was at a given point in time when it was backed up, picking and choosing individual files to restore. Snapshots allow you to perfectly restore each volume to its exact state at the time of any completed backup.

Snapshots help Retrospect keep track of the volumes to which a file belongs. When Retrospect first backs up a volume to a new Backup Set, it copies the selected files and saves a Snapshot. When it subsequently backs up other volumes, it does not copy files that exactly match files already in the Backup Set. However, they are still noted in each volume's Snapshot. This efficient storage saves backup media by not redundantly copying exactly matching files.

You can retrieve Snapshots from media if you want to restore a volume, folder, or file as it was at any given backup.

Because a Snapshot represents a volume at a specific point in time, you cannot use a Snapshot to find multiple versions of a file throughout different backup sessions on different dates. However, Retrospect does provide an easy way of doing this, which is explained in "Restoring by Search" on page 78.

RETROSPECT AND CLIENTS

The Retrospect application can back up any volume that can be accessed from the Windows Explorer or can be assigned a drive letter, whether it is a volume shared over a network or a drive connected directly to your computer.

Retrospect Clients can extend the backup and restore capabilities of Retrospect to other computers on your network. A computer equipped with Retrospect Client software is known as a Retrospect client computer, or simply a client. Retrospect can back up clients on the network without the need for installing file servers, starting file sharing, or mounting volumes.

You could back up other computers on your network using Microsoft Networking, but this requires careful configuration of sharing, users, and permissions. Using Retrospect Client software to back up the same computers is much simpler: you install the client software once, then if that computer is turned on (even if no one is logged in) you can back it up over the network.

HARDWARE

- **HARDWARE OVERVIEW**

- **COMMUNICATION TECHNOLOGIES**

- **SEEING YOUR BACKUP DEVICES**

- **CD/DVD DRIVES**

- **REMOVABLE DISK DRIVES**

- **HARD DISK DRIVES**

- **TAPE DRIVES**

- **TAPE LIBRARIES**

- **REMOVABLE STORAGE MANAGER**

- **MEDIA LONGEVITY AND STORAGE**

- **MULTIPLE BACKUP DRIVES**

- **NETWORK ATTACHED STORAGE (NAS) DEVICES**

This chapter explains the device communication technologies used by Retrospect and describes how to use Retrospect with your backup device. If you are already familiar with SCSI, Fibre Channel, iSCSI, ATAPI, FireWire, and USB, you can skip the explanations and read the sections that apply to your particular hardware setup and backup device.

HARDWARE OVERVIEW

Retrospect uses hardware intensively. Its purpose is to transfer large amounts of data between a source volume, such as a hard disk, and a backup device, such as a tape drive, as efficiently as possible. If these hardware systems do not work correctly, Retrospect cannot properly back up your data. For this reason you should understand how your hardware functions and how it relates to Retrospect.

Tqzkq maintains an extensive laboratory devoted to testing Retrospect with different backup devices. Nothing taxes storage devices more than backups, so if there is a problem, Tqzkq's intensive testing will most likely find it. Device manufacturers supply Tqzkq with pre-release versions of their devices so Tqzkq can identify problems before the devices are made available to the public. Refer to the Tqzkq Retrospect web site for the latest compatibility information and more specific details on supported devices.

If you have problems with Retrospect and your backup devices after you have confirmed you have a valid hardware and software installation, refer to Chapter 11 • Problems and Solutions.

COMMUNICATION TECHNOLOGIES

Retrospect communicates with hardware devices using a number of different methods. This section describes the most common methods and how they interact with Retrospect.

SCSI

SCSI (Small Computer System Interface) is a specification of mechanical, electrical, and functional standards that lets a computer connect and communicate with peripheral devices such as hard drives, tape drives and libraries, and scanners. You can add SCSI capability to your computer with a SCSI host adapter.

SCSI connects a computer with peripherals by linking one or more devices with SCSI cables plugged into SCSI ports. The devices are connected serially—one after the other—in a simple layout known as a daisy chain. Each device must have its own unique identifying SCSI address, or ID. (You set a device's ID number on the device itself.)

Both ends of a SCSI chain must be "terminated" to maintain the integrity of communication signals on the chain. This is done with a terminator, a device that attaches to an open SCSI port and acts as a plug or stopper. Most SCSI cards have built-in termination, so you only need to worry about terminating the other end of your SCSI chain. If you have an internally terminated or self-terminating SCSI device, it should be the last device of the SCSI chain (that is, at the end and the furthest device from the computer). To find out the termination requirements for your specific hardware setup, refer to your SCSI card's documentation and the documentation that came with each peripheral device.

The IDs on your chain do not have to be sequential or in a particular order; the SCSI chain is not affected by the order as long as no devices share the same number.

NOTE: To ensure proper operation of your SCSI devices, always turn on each SCSI device in your chain before you turn on your computer, and do not turn them off until after you shut down your computer.

iSCSI

iSCSI is a storage networking standard that allows SCSI commands to be sent over Internet Protocol (IP) networks. Retrospect supports iSCSI tape drives and libraries, as well as iSCSI disk arrays.

NOTE: Tqzkq recommends using the latest version of the Microsoft iSCSI Software Initiator.

Fibre Channel

Fibre Channel is a serial data transfer architecture designed for storage devices that require very high data transfer rates. Fibre Channel combines the best features from SCSI and IP network transfer protocols.

Retrospect supports fibre channel tape drives and tape libraries using three different topologies:

- Point-to-point: Connects the backup computer directly to the Fibre Channel tape library using a dedicated cable.
- Arbitrated loop (FC_AL): Connects up to 126 devices or nodes in a single, continuous loop or ring.
- Switched fabric: The most complex topology, switched fabric can be used to connect up to 16 million nodes.

NOTE: For FC_AL and switched fabric, Retrospect does not lock the device from other applications or share the device properly. It is the responsibility of the network administrator to ensure that only one copy of Retrospect has full access to the fibre channel storage device.

Retrospect is not designed to share a fibre channel library. To share a fibre channel library between multiple copies of Retrospect, choose a library that can be partitioned into multiple smaller virtual libraries and assign a partition to each Retrospect backup server.

ATAPI

ATAPI (ATA Packet Interface) is a standard for connecting peripheral devices such as CD/DVD drives and tape drives to a computer's IDE interface.

All ATAPI devices are connected internally on the IDE bus. There may be one or two devices per channel, numbered 0 and 1, known as the master device and the slave device respectively.

(ATAPI device numbers are set with jumpers or special cables.)

FireWire

FireWire is a specification of mechanical, electrical, and functional standards which lets a computer connect and communicate with storage devices, such as hard disks and removable disk drives, and other peripheral devices, such as scanners and video camcorders. FireWire is also known as i.LINK or 1394, from its official IEEE 1394 specification.

FireWire connects a computer with peripheral devices by linking as many as 63 devices with special FireWire cables plugged into FireWire ports. FireWire is hot-pluggable, so, in most cases, you do not have to shut down devices to add or remove them, nor do you have to restart your computer. FireWire is capable of extremely fast transfer rates.

Retrospect needs special software drivers to support some FireWire devices. For installation and configuration information and to determine which software is required for your FireWire device, refer to the documentation that came with your device.

USB/USB 2.0

USB (Universal Serial Bus) is a specification of mechanical, electrical, and functional standards which lets a computer connect and communicate with input devices, such as keyboards and joysticks, and peripheral devices, such as storage devices and scanners.

USB/USB 2.0 connects a computer with peripheral devices by linking up to 128 devices with special USB cables plugged into USB ports.

Retrospect needs special software drivers to support some USB devices. For installation and configuration information and to determine which software is required for your USB de-

vice, refer to the documentation that came with your device.

NT Passthrough

For Windows NT/2000/XP/Server 2003 operating systems, Retrospect communicates directly with tape and CD/DVD drives using NT Passthrough.

ASPI

For Windows 98/Me operating systems, Retrospect requires ASPI (Advanced SCSI Programming Interface) software to communicate with tape and CD/DVD drives.

Retrospect automatically installs Adaptec Corporation's ASPI software on Windows 98/Me systems.

SEEING YOUR BACKUP DEVICES

To see a list of the backup devices available to Retrospect, click Configure>Devices from the navigation bar, then click the Environment tab in the Storage Devices window. Retrospect displays all ID numbers and their connected devices, if any.
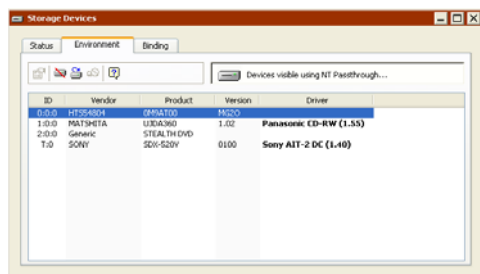
For each address, Retrospect lists the device ID, vendor ID, product ID, firmware version, and Retrospect driver.

If the device has been qualified by Tqzkq for use with Retrospect or the device is "recognized", the driver is identified in boldface. Recognized devices that are not listed as "qualified" on the

Tqzkq Retrospect web site will work fine with the listed driver under most circumstances.

To determine if your device is qualified, refer to the Support & Hardware section of www.tgvtqur gev.com. You can also check the web site to see if Tqzkq has released a Retrospect Driver Update (RDU) for your device.

Retrospect does not have its own drivers for removable disk drives because it can already communicate with them through the operating system.

When You Can't See Your Backup Device

All backup devices that are properly connected to the backup computer should also appear in the Windows Device Manager. If you cannot see the device, refer to its documentation for information on setting it up properly.

If the device you can't see is an internally connected ATAPI device, make sure the cable is firmly connected and it is correctly set as either the master or slave device, or cable select if the computer supports it.

Also make sure your computer's BIOS is set to correctly enable all devices connected to the IDE bus. Refer to the documentation that came with your computer for more details.

For SCSI devices, make sure each device is turned on, the cables are securely connected, each device has a unique ID, and the SCSI chain is properly terminated. Do not rearrange devices on a SCSI chain unless each device and the computer itself are all turned off.

If your SCSI chain is not properly connected and terminated, or if there is an ID conflict, many different problems can result. The most harmless problem would be a device that does not appear in the device status list. A more serious—yet subtle—problem could be a communication failure between the backup

computer and the backup device, leading to data loss. The most serious problem would be damage to your computer or SCSI devices on the chain.

Special Considerations for Windows 98/Me

If you are backing up to tape or CD/DVD under Windows 98 or Me, you must have ASPI installed. The Retrospect installer automatically installs or updates ASPI to the correct version. It is possible that an application installed after Retrospect altered the ASPI version.

First, make sure ASPI is installed correctly on your Windows 98 or Me computer. Run the ASPI check utility (ASPICHK.EXE) from the Retrospect folder. If any ASPI component is a version earlier than 4.60, run the ASPI installer (ASPIINST.EXE) from the Retrospect folder to update it.

Toolbar Commands for Seeing Devices

The Environment tab's toolbar has the following commands for seeing devices:

Ignore ID: If you select a device and click Ignore ID, Retrospect will not scan that ID when Retrospect is next opened after you quit. This may be useful if you are not backing up to your CD/DVD drive and want to use it to play music while you are backing up. It is also a good way to ignore devices on a Fibre Channel or iSCSI network that you don't want the backup computer to see.

Don't Ignore ID: To make Retrospect recognize a previously ignored ID, select the ID and click Don't Ignore ID. Retrospect will scan that ID when Retrospect is next opened after you quit.

Refresh: Clicking this button forces Retrospect to scan for devices and display any changes since the window was initially opened.

Configure CD/DVD Drive: If you select a CD/DVD drive and click this button, you can create (or delete) a custom configuration for your CD/DVD drive. See "Configuring CD/DVD Drives" on page 35 for more information.

CD/DVD DRIVES

With Retrospect, you can back up to and restore from CD/DVD drives. Tqzkq's hardware lab qualifies many, but not all, CD/DVD drives. For a list of qualified drives, see www.tgvtqurgev.com.

NOTE: The list of qualified drives includes a number of double layer DVD drives for use with DVD+R DL and DVD-R DL media.

If your drive is not qualified, Retrospect may still be able to support it. See "Configuring CD/DVD Drives" on page 35 for more information.

When Retrospect is executing a script unattended and requires a new disc, it will automatically use any disc in the drive that is erased or has the correct name.

New, blank CD-R, CD-RW, DVD-R, DVD-RW, DVD+R, or DVD+R DL media is considered erased and will be used. New DVD+RW media will be prepared by Retrospect and then used. Previously recorded CD-R, DVD-R, DVD-R DL, or DVD+R media cannot be erased and thus cannot be used by Retrospect.

Because a disc with any recorded data will not be used by Retrospect in unattended operations, it is a good idea to prepare rewritable media ahead of time by erasing CD-RW, DVD-RW, or DVD+RW discs containing unwanted data. See "Toolbar Commands for Discs" on page 35.

WARNING: You cannot restore data for CD/DVD discs unless you have a *writable* disc drive.

Recordable and Rewritable Media

CD-R, DVD-R, DVD+R, and DVD+R DL discs are write-once media which cannot be erased. Use care when choosing your CD/DVD Backup Set names and when deciding which files to back up.

CD-RW, DVD-RW, and DVD+RW discs are rewritable and can be recorded over and over like removable disks. There is a limit to the number of rewrites, but you are not likely to encounter it with Retrospect.

Tqzkq uses the term "disc" to refer to a recordable disc used in a CD-R, CD-RW, DVD-R, DVD-R DL, DVD+R, DVD+R DL, DVD-RW, or DVD+RW drive. These drives all work nearly the same with Retrospect, though they may use different media. The difference is that data on "R" discs cannot be erased, while "RW" discs can be erased in rewritable drives and reused by Retrospect. Rewritable discs are, of course, also recordable.

Retrospect can use any media supported by a given drive. Different brands, speeds, and types of media vary greatly. For best results, use high-quality media. Some drive manufacturers recommend or require particular brands of media with their drives, while some do not support using high-speed media. Check with your drive manufacturer for media recommendations.

TIP: For maximum performance and reliability, use DVD+R, DVD+R DL, or DVD+RW media if your drive supports it.

Formatting discs with other programs prior to backup is neither necessary nor recommended. Use only unformatted or erased discs.

NOTE: Backup discs created by Retrospect are accessible only by Retrospect or other Retrospect Backup products, and only with supported CD/DVD devices. The discs do not mount on the desktop for use with the Windows Explorer or other software.

Viewing Disc Status

You can use Retrospect to view information about CD/DVD discs that you want to use, or have used, for backups.

Before viewing disc information, make sure the device you want to use is listed in the Storage Devices window. If the device you want does not appear in the window, see "Seeing Your Backup Devices" on page 32.

NOTE: Retrospect requires the exclusive use of the CD/DVD drive and it will first eject any loaded, previously recorded (finalized) CD-ROM or audio disc from the drive. The drive is then reserved for Retrospect's exclusive use until Retrospect quits.

To view disc status:

1. Insert the disc in the drive.

NOTE: When you insert a disc in a CD/DVD drive, the operating system or other software may ask how you wish to prepare or format the disc. Always ignore formatting prompts and exit these windows, as you should not prepare backup discs with anything but Retrospect.

2. Click Configure>Devices.

The Storage Devices window displays.
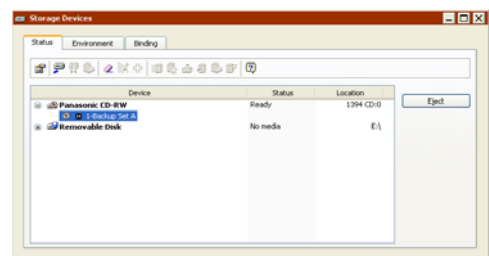
Once a disc is loaded, its status appears:

Ready indicates the disc contains Retrospect data.

Erased indicates an empty disc, ready for use by Retrospect.

Write Protected means the disc is locked or full.

Content Unrecognized means the disc is not empty, but does not contain valid Retrospect data. (see "Content Unrecognized" on page 333).

Wrong Version may mean the drive's firmware is not supported. Or, it may mean the inserted disc was written to by Retrospect for Macintosh. Retrospect for Windows cannot read such discs.

Incompatible indicates that the drive does not support the media that is inserted, or that media type was not used when creating a custom configuration for the drive.

Hardware Error indicates a device error has occurred.

Damaged Disc indicates that the disc was damaged during the previous backup. You may not be able to append to this disc.

Running and Busy indicates the drive is busy.

No Media indicates there is no disc in the drive.

Toolbar Commands for Discs

The Storage Devices window toolbar includes a number of commands for use with discs:

Properties displays information about the disc drive. If a disc is inserted, the Properties window also displays information about it, including whether or not it is a member of a Retrospect Backup Set and its format.

Eject unloads the selected disc from its drive.

Erase erases the contents of the selected rewritable disc. This command is not available with recordable-only discs.

NOTE: When you erase a DVD+RW disc, retrospect asks if you want to do a short or long erase. Short erase performs a fast rewrite of the disc's header. Long erase performs a multi-hour erase and conditioning cycle.

Configuring CD/DVD Drives

Retrospect includes built-in recognition for many CD/DVD drives. For drives that are not recognized, you can create a custom configuration.

NOTE: Custom configurations are not qualified through Tqzkq's rigorous Hardware Certification process, but successful configurations are supported.

During the custom configuration process, Retrospect asks you to insert a blank disc. This disc is used to run a series of tests. Make sure to insert the type of disc (e.g., DVD+RW) that you want to use for backups. After Retrospect finishes configuring the drive for one type of disc, you will have the opportunity to run the tests again with additional media types.

NOTE: It is only necessary to configure the drive with the type of media that will be used for backup.

After creating a custom configuration, you should perform a backup with verification turned on to ensure that Retrospect works properly with the device.

NOTE: When custom configuration is run using write-once media, that media cannot be used for other operations.

Automatic configuration

If the backup computer is not connected to a supported tape or CD/DVD drive, but is connected to an *unrecognized* CD/DVD drive, the CD/DVD configuration dialog automatically appears when you click Configure>Devices or perform another operation that requires a backup device.

To create a custom configuration for the drive click Configure and follow the on-screen prompts. To skip configuration and prevent the

dialog from appearing again, click Ignore. To skip configuration now, but allow the dialog to appear again next time, click Cancel.

Manual configuration

In some rare cases, you may want to create a custom configuration that overrides Retrospect's built-in recognition. You should use this procedure only if you are experiencing difficulty backing up to a CD/DVD drive, or if you are directed to do so by Tqzkq Retrospect Technical Support. While customization may improve communication between Retrospect and the drive, it may not.

In the navigation bar, click Configure>Devices. Click the Environment tab, select the CD/DVD drive you want to reconfigure, then click the Configure CD/DVD button in the toolbar. In the dialog that appears, click Configure, then follow the on-screen prompts to create a custom configuration for the drive.

Deleting a custom configuration

If you created a custom configuration for a CD/DVD drive and you continue to have problems, or your problems get worse, delete the custom configuration.

In the navigation bar, click Configure>Devices. Click the Environment tab and select the CD/DVD drive you want to reconfigure. Right-click it and choose "Configure CD/DVD Drive". In the dialog that appears, click Delete to remove the selected device's custom configuration and use Retrospect's built-in support, if available. Click OK to confirm deletion.

NOTE: Retrospect cannot back up to a CD/DVD drive for which it is has *no* configuration (custom or built-in).

REMOVABLE DISK DRIVES

Removable disk drives use media that can be accessed from the Windows Explorer. This in-cludes Zip, REV, SuperDisk, DVD-RAM, and MO. You must be able to copy files to and from the disk in the Windows Explorer to use a removable disk drive with Retrospect.

NOTE: Before using Retrospect to back up to a removable disk you should be familiar with the procedures to insert, format, erase, and eject disks.

Choosing the Backup Set Type

A removable disk drive can be the destination for both file Backup Sets and disk Backup Sets. There are some important differences between these two types of Backup Set:

• A disk Backup Set can grow continuously by spanning multiple removable cartridges or disks, just as a CD/DVD Backup Set can span multiple discs. A file Backup Set cannot grow beyond the available space of its single disk or cartridge.

• Removable disks used as part of a disk Backup Set must be erased before you can use them. Removable disks used as part of a file Backup Set do not have to be erased, and the disk can store and access files other than the Backup Set data files.

Viewing Removable Disk Status

You can use Retrospect to view information about removable disks that you want to use, or have used, for backups.

To view disk status:

1. Click Configure>Volumes.

The Volumes Database displays.

2. Insert a disk into the drive.

Once the disk is loaded, it appears in the Volumes Database with its drive letter next to it.

Preparing Removable Disks for Use

It is a good idea to prepare removable disks for use ahead of time by erasing or reformatting them, then adding them as members of a Back-

up Set. When Retrospect is executing a script unattended and requires additional storage for the disk Backup Set, it will automatically use a disk that was previously added to the Backup Set.

After formatting or erasing disks as described in "Formatting and Erasing Removable Disks" on page 37, you can add them to disk Backup Sets as described in "Adding a Disk to a Backup Set" on page 260.

Formatting and Erasing Removable Disks

Before you use an unformatted removable cartridge or similar disk with Retrospect, you must first format the disk from the Windows Explorer or a formatting utility.

NOTE: For removable cartridges such as Zip, REV, SuperDisk, DVD-RAM, or MO, format with the software that came with your drive.

It is a good idea to format all of your cartridges using the same formatting method.

TIP: For Windows NT/2000/XP, to avoid long delays while Retrospect erases disks, format your cartridges as NTFS volumes.

To erase removable disks, click Configure> Volumes from the Retrospect navigation bar. Select the disk to erase and click the Erase button on the toolbar.

Toolbar Commands for Removable Disks

Properties displays information about the removable disk drive. If a disk is inserted, the properties window also displays information about it, including whether or not it is a member of a Retrospect Backup Set and its format.

Eject unloads the selected medium from its drive.

Erase erases the contents of the selected disk.

HARD DISK DRIVES

Retrospect supports hard disk drives as a backup destination. This includes internal and external hard disks directly connected to the backup computer, and hard disks served over the network. To use a hard disk with Retrospect, it must be accessible through the Windows Explorer, since Retrospect uses the file system, not custom drivers, to communicate with hard disk drives.

To see the hard disks available for use with Retrospect, click Configure>Volumes.

The main drawback of using a fixed hard disk as a backup device is that it does not have removable media for off-site storage and media rotation. ("Backup Strategies" on page 224 describes these important aspects of safe and secure backups.) "Hot-swapable" and removable drives are more flexible in these respects.

Choosing the Backup Set Type

A hard disk drive can be the destination for both file Backup Sets and disk Backup Sets. There are major differences between these two types of Backup Set. Disk Backup Sets provide the maximum flexibility and performance because they can:

• Span multiple disks, including network volumes

• Include the option to automatically groom disks to reclaim disk space

• Provide the best support for backing up to NAS devices and servers

• Use the same Backup Set as the destination in one operation while, at the same time, as the source for one or more additional operations.

• Support User Initiated Restore (UIR), if you have the UIR add-on.

In addition, disk Backup Sets do not have the file size limitations inherent in a file Backup Set.

When saved on hard disks, both file Backup Sets and disk Backup Sets can store and access files other than the Backup Set data files.

Preparing Hard Disks for Use

It is a good idea to prepare disks for use ahead of time by adding them as members of a Backup Set. When Retrospect is executing a script unattended and requires additional storage for the disk Backup Set, it will automatically use a disk that was previously added to the Backup Set.

To add a disk to a Backup Set, see "Adding a Disk to a Backup Set" on page 260.

Disk Grooming

By default, when a disk that is a member of a disk Backup Set becomes full (or uses all the disk space you allotted), Retrospect asks for a new disk so it can continue to copy files and folders.

If you would rather continue to use the existing disk, you can use Retrospect's grooming options to reclaim disk space by deleting older files and folders to make room for new ones.

Once disk grooming is enabled and you specify a grooming policy (or use Retrospect's policy), Retrospect automatically deletes older files and folders (based on the policy) when it needs more space. For more information on setting disk grooming options in the Backup Set Creation Wizard, see "Grooming Options for Disk Backup Sets" on page 254.

WARNING: Grooming deletes files and folders. These files and folders cannot be recovered. Before enabling grooming, make sure you have a backup policy that protects your critical files and folders.

You can change or turn off a disk Backup Set's grooming options at any time. If you want to protect backups from specific points in time, you can "lock" them to prevent Retrospect from grooming them. You can also select specific Snapshots not groomed by policy, to delete from the Backup Set. See "The Snapshots tab" on page 257 for more information.

Grooming is useful as part of a staged backup strategy. See "Staged Backup Strategies" on page 227 for more information.

TAPE DRIVES

Retrospect supports most tape drives without requiring the installation of additional software. For a list of supported tape drives, see www.tgvtqurgev.com.

Unlike random access devices such as hard drives, removable disk drives, and CD/DVD drives, tape drives are sequential access devices. Since the data reading mechanism cannot immediately go to the correct data position on the media, a tape drive accesses data more slowly than a disk drive (or similar random access device). It is just like fast-forwarding a music cassette to find your favorite song.

Sequential access media is relatively inexpensive, has large capacity, and has a good sustained data transfer rate. Thus, tapes are particularly well suited for backups.

When you use Retrospect to back up a volume to a tape, the data is written sequentially from the beginning of the tape to the end. When you add backups to the tape, the data is appended where the previous data ends, until the tape runs out.

Neither the backup computer nor Retrospect will mount a tape or map it to a drive letter when you put it in the drive, so do not expect the tape to appear on your Windows desktop. Though

the technology exists to let you map a tape as a volume and use it like a disk, you probably would not want to do this for regular backups because of the performance issues discussed previously. Retrospect's system for backing up and restoring files to and from tapes is far more powerful, efficient, and reliable.

Tape Capacity

The actual amount of data that will fit on a given tape will vary due to many factors. A tape's capacity can be greatly influenced by the relative speeds of the backup computer and the tape drive.

If you back up a slow source (for example, a slow computer, a slow hard drive, or a shared volume on a network) to a fast tape drive, the tape capacity is reduced by the source's inability to supply a steady flow of data to the tape drive. (This is like dictating to an audio cassette recorder; you can record more words if you speak quickly without pauses, but when you take a breath you are wasting tape because the recorder is still going, recording silence.) When the tape drive runs out of data while backing up, it must stop writing data, reposition the tape, and resume writing at the correct section of the tape. Each reposition reduces the capacity of the tape, and excessive repositioning can lead to accelerated device wear.

Do not be surprised if your tapes end up with less than their advertised capacities. Some tape drives are represented as being capable of higher capacities than the drives normally achieve in day to day use. The representations refer to the amount of data *before* it gets compressed by a tape drive with hardware compression capability—and they often assume generous compression rates.

Compression

Compression, which can be done by Retrospect or a capable tape drive, conserves space on media by reducing the size of the data being stored. Compression does not actually increase the me-

dia capacity—a given disk or tape can only hold a certain amount of data. Compression squeezes the original data to a more compact size before the data is put on the tape, allowing you to fit more of your files on a given tape.

Hardware data compression is extremely common on tape drives. Retrospect uses a drive's hardware compression whenever possible, automatically turning off Retrospect's software compression option if necessary.

TIP: It is faster to let the hardware compress the data than to have Retrospect compress it.

The amount of compression achieved varies depending on the type of data being backed up. Text files generally compress well, while applications and system files do not. Compression typically reduces data to half its original size.

Retrospect disables hardware compression when you use encryption because encrypted data compresses poorly. If you need to use encryption and compression together, use Retrospect's software compression option. Retrospect then compresses the data before encrypting it, which is not possible when hardware compression is used.

Tape Drive Mechanisms

Though you may buy your tape drive from one of many companies, the drive is actually built around a mechanism from one of several manufacturers. Typically, companies purchase bare mechanisms from manufacturers, put them in their own cases and packaging, and support the products with their own staffs.

Popular types of tape mechanisms available are AIT, DAT, DLT, LTO/Ultrium, S-AIT, Travan, and VXA. Robotic tape libraries are available for several types of these drive mechanisms.

High speed, large capacity tape drives such as AIT, DLT, LTO/Ultrium and S-AIT require a high performance environment. Best speed and

capacity results are achieved with a fast computer processor. The most important performance factor is the speed of the source volume. If the source is too slow, the drive must frequently stop to reposition the tape while waiting for additional data. If the drive repositions too often, copy performance will decrease dramatically.

TIP: A staged backup strategy that involves backing up to disk, then transferring the backup to tape can help improve overall performance when backing up to tape. See "Staged Backup Strategies" on page 227.

AIT

Eight millimeter drives using Advanced Intelligent Tapes (AIT, AIT-2, AIT-3, and AIT-4) are among the fastest tape drives available. Their mechanisms can store 12 to 200 GB of uncompressed data at very high speed when used under optimal conditions.

DAT

DAT drives span the gap between entry-level tape drives such as Travan and higher-end products such as DLT and AIT. Each compact DAT cartridge, containing a length of 4 mm wide tape, holds about 2 GB (DDS-1), 4 GB (DDS-2), 12 GB (DDS-3), 20 GB (DDS-4), 36 GB (DAT 72), or more depending on how much your files are compressed. Speeds range from 6 MB per minute with older DDS-1 drives to 150 MB per minute with newer DAT 72 drives.

DLT

DLT and Super DLT drives are among the fastest tape drives available. Their mechanisms offer exceptional performance and 2.6 GB to 300 GB uncompressed capacity when used under optimal conditions.

LTO Ultrium

Ultrium tape drives are among the fastest and largest capacity tape drives available. The Ultri-um format was created by the LTO (Linear Tape Open) consortium. Ultrium-1 tapes offer an uncompressed capacity of 100 GB. Ultrium-2 tapes offer an uncompressed capacity of 200 GB. Ultrium-3 tapes offer an uncompressed capacity of 400 GB.

S-AIT

Super AIT (S-AIT) drives are among the highest capacity tape drives available. S-AIT tapes offer an uncompressed capacity of 500 GB.

Travan

These tape drives have uncompressed capacities of 1.5, 2, 4, 10, or 20 GB, depending on the tape cartridge used. Travan "NS" (Network Series) drives include hardware compression.

VXA

VXA drives provide tape technology that is reliable and relatively inexpensive for small- to medium-sized environments. VXA formats data in packets, operates at variable speed, and can read data multiple times in a single pass of the tape. A VXA-1 tape can store 33 GB of uncompressed data. A VXA-2 tape can store 80 GB of uncompressed data.

Tape Alert Support

Many tape drives and libraries support Tape Alert messages. These devices generate Tape Alert messages to report hardware errors, There are three categories of alerts:

- Information
- Warning
- Critical

Retrospect supports Tape Alert in three ways. It:

- Displays a dialog box describing the nature of the error.
- Logs the error in the Activity Monitor's Events tab. See "Events Tab" on page 158.

• Logs the error in the Operations Log. See "Viewing the Operations Log" on page 231.

You can enable/disable this behavior for any tape drive or library that is accessible from the backup computer and supports Tape Alert.

NOTE: Retrospect does not automatically enable Tape Alert for most tape drives. You can enable it manually as described below.

To enable/disable Tape Alert:

1. Click Configure>Devices from the navigation bar.

2. Click the Status tab.

3. Select a tape drive or library and click the Properties button ![icon] in the Storage Devices window's toolbar.

4. Click the Tape Alert button ![icon] to enable or disable Tape Alert.
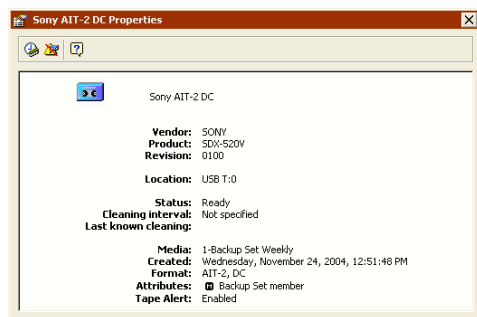
NOTE: If your tape drive does not support Tape Alert, the button is not available.

The Properties window updates to display your selection.

WORM Tape Support

As a result of new compliance regulations and other factors, many tape drives and libraries now support WORM (Write Once, Read Many) tapes.

As the name suggests, WORM tapes cannot be erased or reused once data is written to them.

Retrospect supports the following types of WORM tapes:

• AIT

• S-AIT

• LTO

• SuperDLT

Retrospect also supports the creation of WORM tapes from normal blank or unused SuperDLT tapes using Quantum's DLTIce feature.

WORM tapes are displayed in Retrospect with a special icon so they are easy to identify. While normal tapes use the blue tape icon ![icon], WORM tapes have a yellow icon ![icon].

WARNING: When using WORM tapes, make sure Retrospect's "Automatically skip to blank media" preference is turned off (which is the default setting). See "Request Preferences" on page 270.

• Working with WORM Tapes

• Creating SuperDLT WORM Tapes

Working with WORM Tapes

Since Retrospect treats WORM tapes differently than normal tapes, Tqzkq recommends that you use WORM tapes exclusively with WORM tape Backup Sets.

When you create a new tape Backup Set using the Backup Set Creation Wizard, you can select a check box to create a WORM tape Backup Set. See "Creating Backup Sets" on page 252.

NOTE: You cannot create a WORM tape Backup Set using the Backup Wizard.

WORM tape Backup Sets are displayed in Retrospect with a special icon so they are easy to identify. While normal tape Backup Sets use the blue tapes icon ![icon], WORM tape Backup Sets have a yellow icon ![icon].

WORM tape Backup Sets are treated differently than normal tape Backup Sets. During an auto-

matic operation (i.e. a scripted operation) that uses a WORM tape Backup Set as the destination, Retrospect will copy files to a WORM tape with the correct name. If it cannot find a WORM tape with the correct name, it will automatically use a blank WORM tape *only*. Retrospect will never automatically add a blank, normal tape to a WORM tape Backup Set.

Similarly, during an automatic operation that uses a normal tape Backup Set as the destination, Retrospect will never automatically add a blank WORM tape (only a blank, normal tape) to the normal tape Backup Set.

You *can* manually add normal tapes to WORM tape Backup Sets and WORM tapes to normal tape Backup Sets from the Media Request window or using Retrospect's Add Member to Tape Backup Set feature.

NOTE: WORM tapes can never be erased or reused, even when they are part of a normal tape Backup Set. Normal tapes can be erased and reused even when they are added to a WORM Backup Set.

Creating SuperDLT WORM Tapes

Quantum tape drives with DLTIce have the ability to create WORM tapes from unused SuperDLTtape II tapes. Retrospect allows you to use this feature with SuperDLT 600 or later tape drives.

To create a SuperDLT WORM tape:

1. Click Configure>Devices from Retrospect's navigation bar.

2. Click the Status tab.

3. Select a tape and click the Format button

![icon] from the Storage Devices window's toolbar.
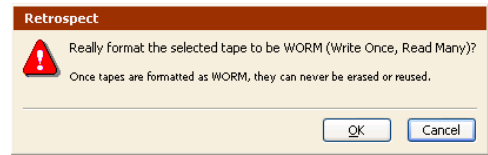
4. Click OK.

WARNING: Once tapes are formatted as WORM, they can never be erased or reused.

Cleaning Your Tape Drive

Regular cleaning of your tape drive is essential for reliable performance. Dirty drive heads are a major cause of tape drive problems and reported media failures. Retrospect may report error – 206 (drive reported a failure, dirty heads, bad media, etc.) in these cases.

Cleaning most tape drives is as simple as inserting a special tape cleaning cartridge and letting the drive clean itself. Refer to your drive's documentation for its manufacturer's cleaning recommendations.

Depending on the capabilities of your tape drive, a number of tape cleaning options are available.

For all tape drives, Retrospect has a Cleaning Interval option. To access this option, click Configure>Devices, select your tape drive in the Status tab, and click the Properties button in the toolbar.
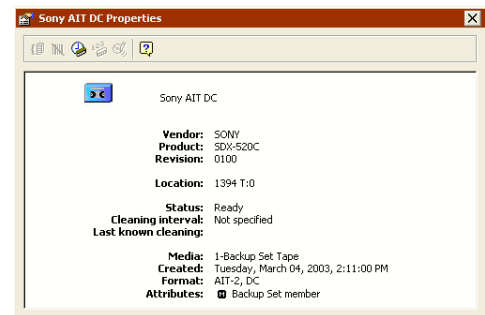
Click the Cleaning Interval button on the Properties window's toolbar and enter the number of hours of drive use between cleanings.
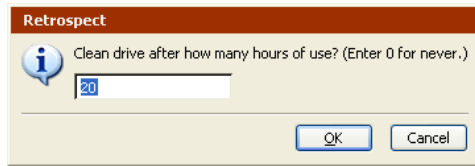
By default, Retrospect enters 20 hours. Enter your drive vendor's recommended cleaning interval and click OK. For standard tape drives, Retrospect adds a note to the log and displays a notification dialog the first time you quit after 20 hours (or whatever number you enter) of use. If you never quit Retrospect, you will never get a reminder.

If you have a tape library that supports barcode reading, and a cleaning tape (with a cleaning barcode label) is loaded in the cleaning slot, Retrospect automatically cleans the drive at the specified interval. If you have a tape library that does not support barcode reading, Retrospect will still automatically clean the drive, as long as you have designated a cleaning slot and inserted a cleaning tape. For more information on tape libraries, see "Tape Libraries" on page 45.

For barcoded cleaning tapes, you can also have Retrospect keep track of how many times the cleaning tape has been used and stop using it after a specified number of times.

To specify the Cleaning Count:

1. Make sure a barcoded cleaning tape is loaded in your tape library, then click Configure>Devices.

The Storage Devices window displays.

2. Select the cleaning tape, then click the Properties button in the toolbar.

3. Click the Cleaning Count button.

4. Enter a number and click OK.

At any time you can see how many available cleanings remain, by checking the Properties of the cleaning tape.
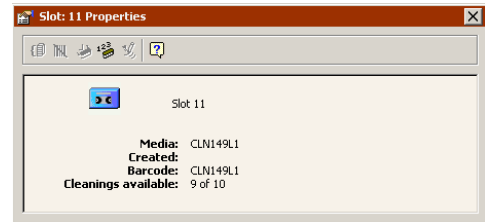
Viewing Tape Status

You can use Retrospect to view information about tapes that you want to use, or have used, for backups.

Before viewing tape information, make sure the device you want to use is listed in the Storage Devices window. If the device you want does not appear in the window, see "Seeing Your Backup Devices" on page 32.

To view tape status:

1. Click Configure>Devices.

The Storage Devices window displays.

2. Insert a tape into the drive.

Once a tape is loaded, its status appears on the Status tab:
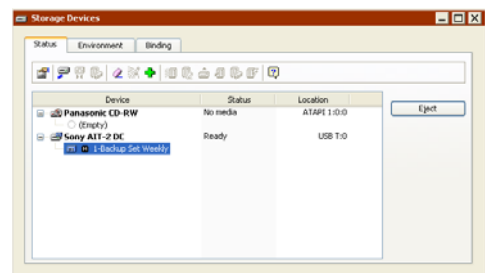
Ready indicates the medium contains Retrospect data or is a member of a Backup Set that is ready for use.

Erased indicates an empty medium.

Content Unrecognized means the tape is not empty, but does not contain valid Retrospect data. Often, this happens when a compressed tape is inserted in a drive without hardware compression abilities. It also happens when you insert a tape written to by other backup software. (see "Content Unrecognized" on page 333.).

Wrong Version may mean the inserted tape was written to by Retrospect for Macintosh. Retrospect for Windows cannot read such tapes. It can also mean the drive's firmware version is not supported by Retrospect.

Write Protected means the tape is locked.

Hardware Error indicates a device error has occurred.

Unloaded usually means a tape is in the drive but is rewound and must be ejected and reinserted to be used.

Running and Busy indicate the drive is busy.

No Media indicates there is no tape in the drive.

Preparing Tapes for Use

When Retrospect is executing a script unattended and requires a new tape, it will automatically use any appropriate tape that is erased or has the correct name. It is a good idea to prepare media for use ahead of time by erasing or formatting tapes.

You can also add tapes to a Backup Set in advance of Retrospect requesting them. For a single tape drive, you can add one tape at a time. For tape libraries, you can select multiple tapes and add them all as members of a Backup Set at once.

To add tapes to a Backup Set:

1. In the Storage Devices window, select the tape(s) to add.
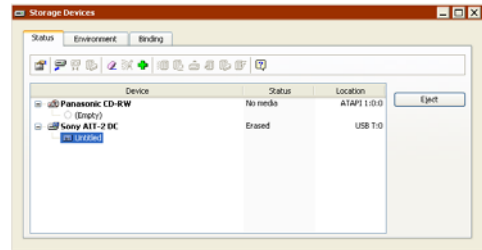
NOTE: You must select blank, erased, or "content unrecognized" tapes. You cannot add tapes that already belong to an existing Backup Set.

2. Click the "Add to Backup Set" button in the Storage Devices window toolbar.

3. Select a Backup Set from the list and click Add.
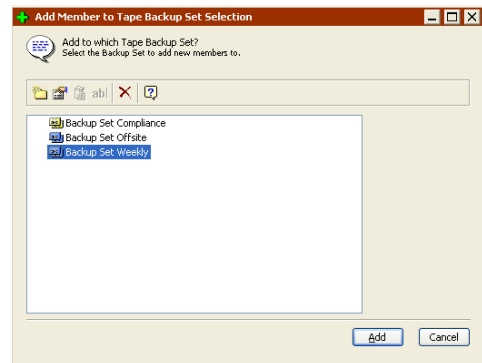
Retrospect may need to erase tapes before adding them to the Backup Set. If a warning dialog displays, click OK to erase the tape(s).

The Storage Devices window displays a name and member icon for each tape that you added.

NOTE: You can also add tapes to a Backup Set from the Backup Set properties window. See "Adding Tapes to a Backup Set" on page 260.

Toolbar Commands for Tape Drives

The following commands for working with tape drives are available on the toolbar.

Properties displays information about the tape drive. If a tape is inserted, the properties window also displays information about it, including whether or not it is a member of a Retrospect Backup Set, its format and the hardware compression setting. The Properties window includes two buttons:

- The Cleaning Interval button 🕐. See "Cleaning Your Tape Drive" on page 42 for more information.
- The Tape Alert button 🔔. See "Tape Alert Support" on page 40 for more information.

Eject unloads the selected tape from its drive.

Retension winds the selected tape forward to the end and back to even out the tension and alignment. (Some types of tapes are retensioned automatically during execution, and cannot be retensioned manually with this command.) You should retension tapes if they have not been used in a long time or if the temperature or humidity of their storage environment has changed significantly.

Clean is only available if you are using a tape library. When you select a drive and click Clean, the library moves the cleaning tape from its storage slot to the drive and begins cleaning. When it's done, the tape is moved backed to its storage slot. See "Cleaning Your Tape Drive" on page 42 for more information.

Erase erases the contents of the selected tape, and—in the case of some tape drive mechanisms—conditions media to be reused.

Format completely reformats the selected tape. This process can be more time-consuming than Erase. It is only supported by certain tape drives. For tape drives with Quantum's DLTIce features, you can use the Format command to create WORM tapes from normal blank or unused SuperDLT tapes. See "Creating SuperDLT WORM Tapes" on page 42.

Add to Backup Set lets you add the selected tape as a member of a tape Backup Set. See "Preparing Tapes for Use" on page 44 for more information.

Additional commands are available for tape libraries. See "Toolbar Commands for Tape Libraries" on page 47.

TAPE LIBRARIES

A tape library (sometimes called a loader, autochanger, or autoloader) is a hardware unit that mechanically moves tapes in and out of its drive mechanism(s) from a magazine or fixed storage slots holding several tape cartridges. Tapes can be arranged in any order and Retrospect will determine which tape it needs to perform an unattended backup. Tape libraries are useful for large-scale network backups because they automatically change tapes when one fills up, limiting downtime. Many tape libraries are available, each using one or more of the many available tape drive mechanisms. For more information, refer to the libraries' manual and the Support & Hardware section of www.tgvtqurgev.com.

NOTE: Tape library support is only available if you have the appropriate license code. Generally, Retrospect SingleServer, Retrospect Multi Server, and Retrospect Small Business Server support tape libraries, while Retrospect Professional does not.

Retrospect supports barcode-reading libraries and manages tape cartridges based on their barcode identification. It displays a tape's barcode in addition to its member name (if any) in media requests, Backup Set properties, Operations Log events, and the Storage Devices window. Retrospect recognizes CLN-coded cleaning cartridges.

Retrospect supports multiple import-export slots to move cartridges within and to and from

the library. Import-Export slots appear in the Storage Devices window. You can drag and drop tapes to and from the import-export slots.

If you have a tape library with multiple drives and the Advanced Tape Support add-on, Retrospect can perform multiple operations using different drives simultaneously. See "Multiple Concurrent Executions" on page 161 for more information.

How Retrospect Works with Tape Libraries

Retrospect works differently with tape libraries depending on whether or not the library supports barcode reading.

Retrospect supports barcode-reading libraries and manages tape cartridges based on their barcode identification. It displays a tape's barcode in addition to its member name (if any) in media requests, Backup Set properties, Operations Log events, and the Storage Devices window. In addition, Retrospect recognizes CLN-coded cleaning cartridges. Barcode support enables Retrospect to quickly scan the storage slots in a library to determine their contents.

If your library does not support barcode reading, Retrospect must scan the library to get the name of each tape. The library inserts each tape in the tape drive, and Retrospect keeps track of the tape names and locations.

WARNING: Each time Retrospect is launched, or the library's door is opened, or the magazine is changed, the library's contents may change, so Retrospect must scan to keep current.

For libraries without barcode support, Retrospect uses a unique feature called "storage slot memory" that speeds up subsequent scans of the library. Each time you exit Retrospect, it records the state of each slot and drive in the library and saves this information as one of ten tables in its configuration file. (The ten tables reflect the ten most recent library scans.)

You can think of saved library tables as a kind of educated guess in the hunt for the correct tape. This method greatly increases the odds of finding a tape on the first attempt if the locations of the tapes in the library's magazine remain relatively constant. If Retrospect cannot find the correct tape using this method, it rescans the library to update the current inventory.

Viewing Tape Library Status

To view a tape library's status, insert a loaded magazine (if applicable) and click Configure> Devices to display the Storage Devices window. Notice how the library, tape slots (including import-export slots), and drives appear in the Status window.
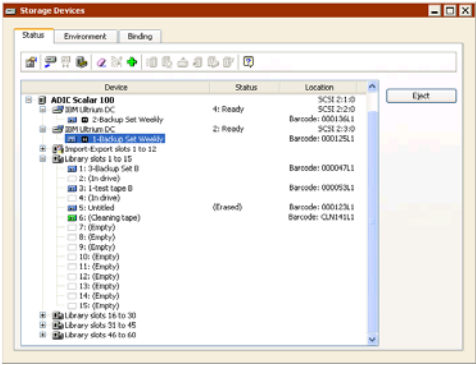
Retrospect displays information about the library, tape drives, and each of the storage slots, including status, location, and barcode. Icons and additional status information indicate the contents of each slot.

Icon	Status or Tape Name	Comments
	(Empty)	The slot has no tape.

Icon	Status or Tape Name	Comments
(icon)	(In drive)	The slot has no tape because it was moved into the drive. This is certain because the library always knows from which slot it has moved a tape into the drive.
(icon)	(Unknown)	The slot has never been scanned by Retrospect.
(icon) (green icon)	(Cleaning tape)	The slot has been designated as a cleaning tape slot by Retrospect. Cleaning tapes use a green tape icon.
(icon)	*Name*	The named tape was in the slot when Retrospect last scanned for tapes, but the status is unverified because the slot's content may have changed since then.
(icon) (blue icon)	*Name [Barcode]*	The named tape was in the slot when Retrospect last scanned for tapes, and is verified because the slot's content could not have changed since then.
(icon) (red icon)	*Name*	There was a media error writing to the tape. Retrospect will not use this tape for automatic executions (scripts). You must manually erase the tape to reuse it.
(icon) (yellow icon)	*Name*	This tape is formatted as WORM (Write Once, Read Many). See "WORM Tape Support" on page 41.

Working with Tape Libraries

From the Storage Devices window, you can move tapes by dragging and dropping their icons. Position the pointer over a tape icon. When the pointer turns into a hand, you can click and drag a tape from slot to slot, slot to drive, drive to slot, or drive to drive. For slot to slot moves, you can selected multiple tapes to move at one time.

Shift-click to select multiple contiguous tapes. Control-click to select multiple non-contiguous tape. You can also select the library itself to select all tapes in the library or select one or magazines to select all tapes they contain.

Many of the Toolbar Commands for Tape Libraries can also be applied to multiple tapes at one time.

Toolbar Commands for Tape Libraries

The Storage Devices window's Status tab toolbar has commands for tapes libraries.

If you select a tape drive that is part of a tape library, its toolbar commands are the same as those for a standalone tape drive. See "Toolbar Commands for Tape Drives" on page 44.

Properties displays information about various attributes of the selected library, including the number of slots the library has and whether barcode scanning is enabled or not. The properties window also includes a toolbar with the Magazine View and Disable/Enable Barcode Scans commands.
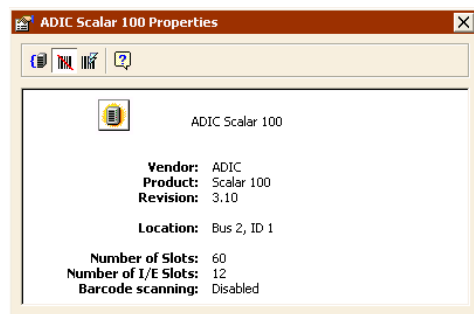
The Magazine View command is most useful for libraries with many slots. It lets you group slots together for easier viewing and slot management in the Storage Devices window. Click the Magazine View button (icon) to specify the maximum number of slots to include in a group and Retrospect organizes the library based on your selection. For example, if your library has

60 slots, and you specify a maximum of 15 slots per magazine, Retrospect creates four magazine containers with 15 slots each. The number you specify does not represent any actual physical grouping of slots or magazines; it is for display purposes only.

If your tape library supports barcode reading, Retrospect automatically uses barcode data to generate the information displayed in the Storage Devices window. You can disable barcode scans by clicking the Disable/Enable Barcode Scans button . You can also click the Clear Barcode Information button to unlink barcode information from all known tapes. This feature should only be used if Retrospect is incorrectly displaying barcode information or tape names, or if directed to do so by Tqzkq Retrospect Technical Support.

Add to Backup Set lets you add tapes in the selected slots as members of a tape Backup Set. See "Preparing Tapes for Use" on page 44 for more information.

Scan Selected cycles through the selected storage slots in the library, moving each tape from slot to drive to learn the name of the tape. You do not need to use this command if your tape drive supports barcodes.

Erase Selected erases each tape in the selected storage slots of the library.

NOTE: If your selection includes WORM tapes, Retrospect skips them when erasing.

Move Selected to Drive moves the selected tapes from their slots to the tape drive(s).

Unload All/Eject Magazine unloads tapes from the library's drive(s) and returns them to their slots. Then, for capable libraries, ejects the library's magazines.

Cleaning Slot designates the selected slot as a cleaning slot. Retrospect will not scan the cleaning slot when it searches for media. If your

library supports barcode reading, Retrospect automatically recognizes a CLN-coded cleaning tape and reserves its slot for cleaning purposes. You can specify the number of cleanings per tape and how often to clean a tape drive from the Properties window for the drive or tape. See "Cleaning Your Tape Drive" on page 42.

Initialize Elements sends the Initialize Element Status command to the library, which forces the library to update the status of all elements. Use this command if you encounter a situation in which the information reported in the Storage Devices window does not match the actual state of the library.

Import-Export Support

Some libraries come with separate ports that are used to load single tapes into and from the library without opening the door. Retrospect uses the term "import-export slot" for this feature, which is also known as "Mail Slot," "I/E element," and "Call Slot." If the import-export slots are present and enabled in a library, Retrospect displays them as separate slots at the top of the list of slots. You can drag and drop tapes from the source drive or any slot onto the import-export slot and the library will move the selected tape to the port. When you place a tape into the port, Retrospect displays "Media Available" next to the import-export slot and you can move it by dragging it to any slot or drive in the library.

Retrospect does not scan import-export slots during unattended operation. Do not place a tape in the import-export slot if you want to use the tape in an unattended operation such as a scripted backup.

Tape Library Media Requests

During immediate and automated operations, Retrospect scans the library, searching for the appropriate media, and loads whichever tape is required. If a new or erased tape is required,

Retrospect will load and use the first one available.

If it cannot find an appropriate tape to use, Retrospect displays the media request window. The operation cannot continue until you insert media.

NOTE: Retrospect does not scan import-export slots during media requests.

Tape Library Media Failures

When Retrospect encounters a media failure, this is a fatal error that stops all operations.

With tape libraries, you can turn on Retrospect's "Use new media automatically after write failure" media handling preference to avoid stopping all operations. If this preference is enabled and Retrospect encounters a media failure, it looks for the next available tape and uses it instead. See "Handling Preferences" on page 269.

REMOVABLE STORAGE MANAGER

Windows 2000, XP, and 2003's Removable Storage Manager allows you to manage tape libraries and other storage devices in conjunction with the operating system's built-in backup utility.

Because this interferes with Retrospect's access of those same devices, Retrospect stops the service by default when it scans for devices. With the service stopped, you can no longer use Removable Storage management. Use Retrospect's Media Handling Preferences to control how Retrospect works with Removable Storage Manager.

Using Retrospect and Removable Storage Simultaneously

If you need the Removable Storage service intact for managing devices other than those used by Retrospect, you can configure Retrospect and Removable Storage in order use both simultaneously.

First, you must prevent Retrospect from automatically stopping Removable Storage Manager. Then, from Windows, you must disable Removable Storage Manager for the devices dedicated to Retrospect.

To set Retrospect Preferences:

1. In the navigation bar, click Configure> Preferences.

2. In the Preferences list box, choose Media> Handling.
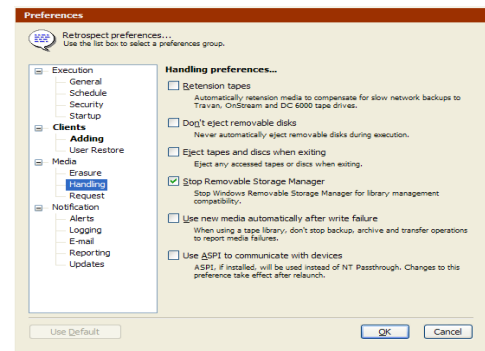
3. Deselect the Stop Removable Storage Manager check box.

4. Click OK.

To set Windows device properties:

1. Open your Windows Removable Storage management console.

2. For each device you want to use exclusively with Retrospect, right-click the device and choose Properties.

3. Click the General tab, then deselect the Enable Library or Enable Drive check box.

For a library, you may have to disable both the library itself and its drive or drives.

4. Click OK and close the management console.

MEDIA LONGEVITY AND STORAGE

Media life depends largely upon how the media is stored and maintained. Proper storage avoids moisture, heat, and particulate contamination, which cause media deterioration, leading to loss of media integrity or loss of data itself.

Magnetic media's worst enemy is moisture. Optical media's worst enemy is heat, which causes distortion, and particulate matter, which causes scratches. Keep media out of direct sunlight and away from heaters. Avoid extreme temperature changes. Airborne particulates such as dust and cigarette smoke can also harm media.

Tapes are unique in that they use lubricant. The tape media is lubricated, and after many passes over the drive's heads, tapes tend to fail because the lubricant has dissipated. You should be able to get a few thousand passes from a tape, but remember that each tape operation involves several passes.

A fire-proof safe in a climate-controlled building is an ideal media storage location. At the very least, keep the media in its original containers inside a cabinet or desk.

MULTIPLE BACKUP DRIVES

During an operation, Retrospect searches available backup devices for the appropriate medium. If the medium fills or Retrospect needs another medium for any reason, it searches available drives. Thus, you can have one drive with the tape Retrospect expects and another drive with an empty tape for when the first tape fills during the night. The drives must use similar mechanisms, such as two Travan drives.

With Advanced Tape Support add-on, Retrospect can work with multiple drives simultaneously. If you have two tape drives, or a tape library with multiple drives, Retrospect can back up data to both drives concurrently

(provided the backups have unique sources). See "Multiple Concurrent Executions" on page 161 for more information.

NETWORK ATTACHED STORAGE (NAS) DEVICES

Retrospect works with Network Attached Storage (NAS) devices in a number of ways. You can run the Retrospect application or Retrospect Client on the NAS device, or you can use the NAS device as the destination to store data for disk Backup Sets.

Backing up to a NAS Device

Retrospect works with a NAS device the same way it works with any other network volume. If you can access the device from Windows Explorer, Retrospect can use it as a destination.

To use a NAS device as a backup storage destination, create a disk Backup Set and select the NAS volume as its media.

Backing up a Windows-based NAS Device

If you are storing a lot of data on a NAS device, it's important to back it up. You can back up a NAS device as a network volume (see "Microsoft Networking Volumes" on page 197), although that is not the best method.

E recommends that you install the Retrospect application or Retrospect Client on the NAS device, then back it up locally or remotely using Retrospect.

In order to run the Retrospect application, the NAS device requires:

- Windows 2000 Server or later with Microsoft Server Appliance Kit; or Windows Storage Server 2003
- Retrospect Single Server or Retrospect Multi Server

In order to run Retrospect Client, the NAS device requires:

• Windows 2000 Server or later with Microsoft Server Appliance Kit; or Windows Storage Server 2003

In addition, the backup computer requires Retrospect Multi Server, or Retrospect Single Server with a server client license, in order to back up the NAS client.

Setting up a Windows-based NAS device to run Retrospect

In order to install and run Retrospect on a NAS device, you need to be able to control the device remotely using Windows Terminal Services or Remote Desktop.

To install Retrospect:

1. Connect to the NAS device using Terminal Services or Remote Desktop.

2. Create a Backup Administrator account on the NAS device and assign it Administrator rights.

3. Switch to the Backup Administrator account from the current account.

4. Copy the Retrospect installer to the NAS device.

5. Install Retrospect.

To set up Retrospect:

1. Connect to the NAS device using Terminal Services or Remote Desktop.

2. Log in using the Backup Administrator account.

3. Launch Retrospect.

The first time you start Retrospect, the Getting Started Wizard runs.

4. In the user account screen, select "Always run Retrospect as the specified user" and enter user, password and domain information.
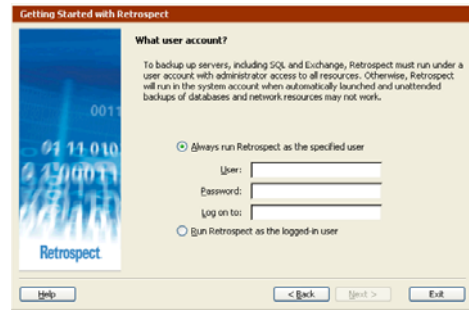
NOTE: This user must have administrator privileges to all network resources, and SQL/Exchange servers you want to access.

For more information about the Retrospect User Account and how to modify login information, see "Security Preferences" on page 265.

5. Click OK.

In order for Retrospect to launch under the Backup Administrator account, even while that session is disconnected, you need to modify Retrospect's Security preferences.

To modify Retrospect's Security preferences:

1. Launch Retrospect on the NAS device.

2. Click Configure>Preferences.

3. Select the Security preference under the Execution heading.
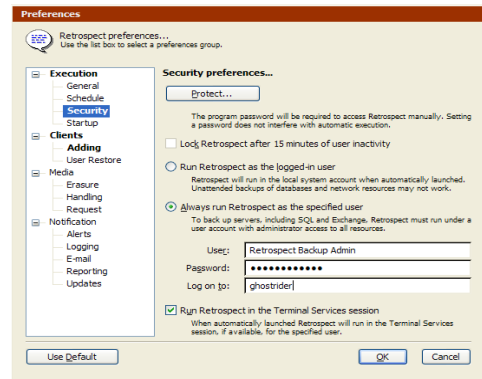
4. Make sure the "Run Retrospect in the Terminal Services session" check box is selected.

Exit and relaunch Retrospect to make this change take effect.

Now, whenever you need to access Retrospect on the NAS device, simply log into the Backup Administrator account.

For Terminal Services/Remote Desktop, the server must also be configured so that a disconnected session will never time out.

To configure the user account:

1. In the Computer Management control panel, select users.

2. Open the Properties for the Backup Administrator account.

3. Click the Sessions tab and select Never in the "End a disconnected session" list box.

To configure the connection properties:

1. Open the Administrative Tools control panel folder.

2. Launch the Terminal Services Configuration Control Panel.

3. Highlight Connections, right-click RDP-Tcp and select Properties.

4. Click the Sessions tab and confirm that the Override User Settings box is unchecked.

If you log out of the Terminal Services session, all running applications will quit, including Retrospect. If Retrospect is running and you want to close the control window, disconnect from the Terminal Services session, but leave the session running. The next time you connect, the same session will be running and Retrospect will be unaffected.

Setting up a Windows-based NAS device to run Retrospect Client

In order to install and run Retrospect Client on a NAS device, you need to be able to control the device remotely using Windows Terminal Services or Remote Desktop.

To install Retrospect Client:

1. Connect to the NAS device using Terminal Services or Remote Desktop.

2. Create a Backup Administrator account on the NAS device and assign it Administrator rights.

3. Switch to the Backup Administrator account from the current account.

4. Copy the Retrospect Client installer to the NAS device.

5. Install Retrospect Client.

Make sure to remember your password, then restart the NAS device.

You can now access the NAS device from Retrospect as described in "Working with Clients" which starts on page 171.

Binding a NAS Device

If Retrospect is running on a NAS device that has multiple network interfaces, you can bind Retrospect to use a specific interface for some or all of its backup clients in order to better manage network traffic.

See "Interfaces" on page 181 for more information.

If Retrospect Client is running on a NAS device that has multiple network interfaces, you can bind Retrospect Client to use a specific interface.

IMMEDIATE OPERATIONS

- **BACKUP**

- **ARCHIVE**

- **RESTORE**

- **DUPLICATE**

- **TRANSFER BACKUP SETS**

- **TRANSFER SNAPSHOTS**

- **CONTROLLING IMMEDIATE OPERATIONS**

Immediate operations are ones that you initiate manually and that execute immediately. Types of immediate operations are: backup, archive, restore, duplicate, and two types of transfer. This chapter describes each of these operations in detail.

If you are a casual user needing only occasional backups, you will be satisfied with immediate operations. However, if you are a network administrator who frequently backs up multiple volumes, you are better off automating these tasks with scripts. Whether you plan to do immediate or scripted operations, this chapter is a good introduction to Retrospect.

BACKUP

This section describes how to perform an immediate backup with Retrospect. The backup procedures described here include all the information you need to know to effectively back up all of your files.

Before you attempt to back up files with Retrospect, ensure that your backup device is properly connected to the computer and that your backup medium (tape, disk, or disc) does not contain valuable data that should not be overwritten.

There are two ways to set up an immediate backup. You can use Retrospect's Backup Wizard, which walks you through the process of setting up a backup, or you can set up the backup on your own in Advanced Mode. Advanced Mode has options that are unavailable in the wizard. For more information see:

- Backing Up in Wizard Mode
- Switching from Wizard to Advanced Mode
- Backing Up in Advanced Mode
- Switching from Advanced to Wizard Mode

In both Wizard Mode and Advanced Mode, Retrospect backs up all selected files during the first backup. In subsequent backups (unless you indicate otherwise), Retrospect backs up only those files that do not already exist in the destination Backup Set (i.e., files that are new or have changed since the last backup). Retrospect calls this Progressive Backup. This means that if you back up frequently, fewer files need to be copied in each backup session and backups will require less time and media.

Backing Up in Wizard Mode

The Backup Wizard provides an easy way to set up and edit immediate backup operations. To start the Backup Wizard, click Backup from the navigation bar, then click the Backup button.

If you have never backed up before (or have previously set up an immediate backup using the wizard), the Backup Wizard welcome screen displays.

TIP: If the Advanced Mode Backup Summary screen displays, click Switch to Wizard Mode.

Welcome Screen

If this is the first time you are setting up a backup, click Next to continue set up using the Backup Wizard. To set up the backup in Advanced Mode, click Switch to Advanced Mode. See "Backing Up in Advanced Mode" on page 61 for more information.
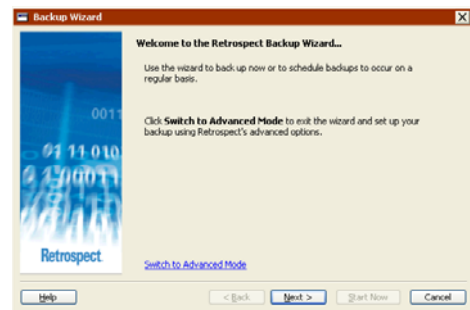
If you have previously set up a backup, the welcome screen displays your current settings. See "Editing the Backup Settings" on page 60 for more information.

Choosing What to Back Up

Click the option button that describes what you want to back up. The options vary slightly depending on what edition of Retrospect you are running.

- **Documents and Settings,** (only available for Retrospect Professional) backs up the Documents and Settings folder, which contains every users' folders, including My Documents, Pictures, Music, Favorites, and Desktop.
- **My Computer**, backs up the local computer.
- **My Computer and computers on my network**, backs up the local computer and all logged in Retrospect Client computers.
- **Only computers on my network**, (not available for Retrospect Professional) backs up all logged in Retrospect Client computers.
- **Let me choose**, allows you to select the drives and folders you want to back up from the local computer, logged in Retrospect Client computers, and network volumes.

Adding Retrospect Clients

If you chose to back up "My Computer and computers on my network" or "Only computers on my network", Retrospect will back up data from all Retrospect Client computers logged in at the time of the backup.

To log in Retrospect Clients now, click Add Clients. For more information on installing, configuring, and logging in clients, see Chapter 7 • Networked Clients.

Choosing Specific Drives or Folders

If you selected "Let me choose" in the "What do you want to back up?" screen, you can now select one or more specific drives or folders to back up.

Click a drive or folder to select it. This deselects any other selected drive or folder. Press and hold the Control key and click a drive or folder to select it without deselecting any current selections. Press and hold the Shift key and click a drive or folder to select all drives and folders listed from the current selection to the Shift-clicked selection.

You can select drives and folders from any of the containers listed in this screen: My Computer, My Network Places, Backup Clients, and Source Groups. You can also select one or more of the containers themselves to back up everything inside.

- To add Retrospect Clients to the Backup Clients container, click Add Clients.
- To add network volumes to the My Network Places container, click Add Network Volumes.
- To display the folders on a drive, select the drive and click Show Folders.

See "Containers" on page 281 for more information.

Choosing File Types to Back Up

Select the check box for each type of file you want to back up. If you select all the check box-

es, all files (except cache files) will be backed up.

NOTE: Some of these options function differently with Windows, Mac OS, NetWare, and UNIX computers. The descriptions below focus on how these options interact with Windows computers. To learn how these options work with other operating systems, see "Built-in Selectors" on page 292.

- **Documents and Settings** backs up files in the Documents and Settings folder, which contains every user's My Documents, Favorites, Application Data, and Desktop folders.

  NOTE: For Windows 9x systems, "Documents and Settings" backs up the "Profiles" folder.

- **Operating System and Applications** backs up system files, including the Windows folder and the System State. Also backs up application files, including everything in the Program Files folder, as well as files with known application extensions (like .exe and .dll) anywhere on the source.

  NOTE: If you choose not to back up "Operating System and Applications", Retrospect modifies some of its default execution options. Retrospect turns off both the "Back Up System State" and "Back up folder security information for workstations" options. See "Windows System Options" on page 244 and

"Windows Security Options" on page 245 for more information.

- **Pictures** backs up all files in the My Documents\My Pictures folder for all users. It also backs up files with common picture file extensions (.jpg, for example) anywhere on the source, except the Windows and Program Files folders.

- **Music** backs up all files in the My Documents\My Music folder for all users. It also backs up files with common music file extensions (.wma and .mp3, for example) anywhere on the source, except the Windows and Program Files folders.

- **Movies** backs up all files in the My Documents\My Videos folder for all users. It also backs up files with common movie file extensions (.mov, for example) anywhere on the source, except the Windows and Program Files folders.

- **Office Documents** backs up Microsoft Office Documents, Microsoft Outlook data, and Adobe PDF files anywhere on the source, except the Windows and Program Files folders.

- **All Other Files**, backs up all files not selected by the other options.

NOTE: The Documents and Settings and Operating System and Applications options are not available if you are backing up a folder.

Choosing the Backup Destination Device

You can store your backup on any device supported by Retrospect, including tape drives, CD/DVD drives, and hard drives. Select one of the following options:

- Tape, CD, DVD
- Hard drives on the local computer or on the network

For Tape/CD/DVD, Retrospect displays the available devices. Select the device to which you want to back up and click Next.

For hard drives, Retrospect displays local hard drives and any network volumes listed in the My Network Places container.

To add a network volume, double-click My Network Places, then navigate to the volume you want to add, select it, and click the Add button. If the volume requires it, enter a login and password and click OK.

NOTE: If you set up Retrospect to log in as a user with privileges to the network volume, you will not be prompted to log in again. See "Security Preferences" on page 265 for more information.

To specify a folder on a local drive or network volume, select it, then click the Browse button. Navigate to the folder you want to back up to and click OK.

Choosing When to Back Up

For immediate backups, select Now.

If you want to set up a backup to run on a schedule, select Later.

The steps to set up a backup to run later are described in "Creating a Backup Script in Wizard Mode", starting with "Choosing When to Back Up" on page 102.

Naming the Backup Set

A Backup Set is a group of one or more disks, tapes, or CD/DVD discs on which your backed up data is stored. When the first piece of media in a Backup Set fills up with data, Retrospect asks for a new one and adds it as a new member of the Backup Set.

Enter a Backup Set name, or use the default name provided by Retrospect. If you have already created any Backup Sets, you can select the "Use Existing" check box and choose a Backup Set from the list box.
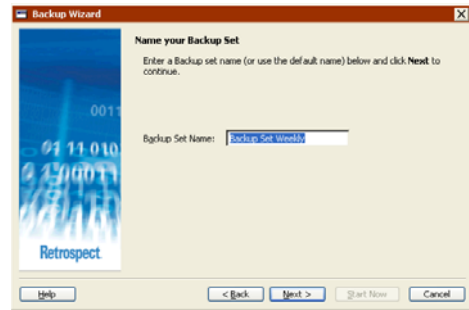
NOTE: The "Use Existing" check box only appears if you have existing Backup Sets.

Setting the Compression Option

Click the "Yes" option button to turn on software data compression for this backup.

Data compression saves space in the Backup Set by compressing files before copying them into the Backup Set. Files are automatically decompressed back to their original state when restored.

The amount of compression savings you can expect depends on the types of files you are compressing. Text files compress substantially; application and system files do not.

Backups (and restores) from Backup Sets using data compression are slower than those that do not.
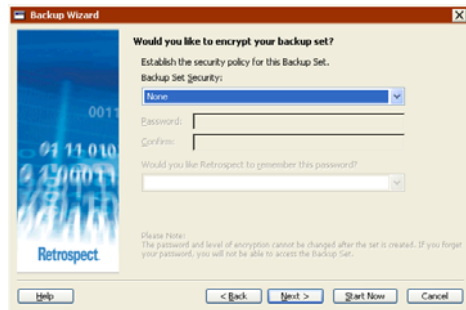
NOTE: When copying to a tape device that has built-in hardware data compression, Retrospect automatically turns off software compression

and always uses hardware compression for best performance.

Setting Backup Set Security Options

This screen allows you to specify a password to restrict access to the Backup Set. You can also choose to encrypt the Backup Set data to provide additional security.

NOTE: Using encryption increases backup time.

Choose an option from the Backup Set Security list box.

- **None**: provides no password protection for the Backup Set and does not encrypt the Backup Set data.
- **Password only**: provides password protection for the Backup Set. Stored data is not encrypted.
- **SimpleCrypt**: provides password protection and encrypts Backup Set data using Retrospect's proprietary encryption format.
- **DES**: provides password protection and encrypts Backup Set data using the Data Encryption Standard.
- **AES-128**: provides password protection and encrypts Backup Set data using the Advanced Encryption Standard (128 bit).
- **AES-256**: provides password protection and encrypts Backup Set data using the Advanced Encryption Standard (256 bit). AES-256 provides the best combination of security and performance.

WARNING: Once a Backup Set is password-protected or encrypted, you *cannot* change these settings. In addition, if you forget your password, you will not be able access the Backup Set.

If you set a password and want Retrospect to remember it under certain circumstances, select an option from the remember password list box.

- **Remember password for any access**: saves the password for use with all immediate and automated operations.
- **Remember password for scripted access** (default): saves the password for use with automated operations only. For example, if the Backup Set is the destination for an overnight backup script, Retrospect will not require the password to be entered manually.
- **Do not remember password for any access**: requires you to enter the password to access the Backup Set in any way. For example, you cannot back up to it or view its properties without entering the password. After you enter the password once, you do not have to enter it again until you quit and restart Retrospect.

NOTE: You *can* change the remember password setting at a later time by modifying the Backup Set's properties. See "Configuring Backup Sets" on page 255 for more information.

Grooming Options for Hard Drive Backups

If you are backing up to a new disk Backup Set that uses a hard drive as its destination, you can tell Retrospect what to do when the hard drive becomes full.

NOTE: You can change or turn off a disk Backup Set's grooming options at any time. See "The Options tab" on page 256 for more information.

- **Ask for a new disk** When the backup drive fills up, Retrospect asks for another hard drive on which to store additional backups. All of your backups on the original hard drive are preserved.

- **Keep only the last _n_ backups**: Specify the number of backups you want to preserve for each source when the backup drive fills up. Retrospect then automatically "grooms" (i.e., deletes) all the other, older backups on the hard drive to make room for new data.

- **Keep according to Retrospect's defined policy**: When the backup drive fills up, Retrospect uses its own grooming policy to delete old backups. At a minimum, Retrospect's policy retains two backups for each source. Retrospect keeps the last backup of the day for each source from the two most recent days on which each source was backed up. If the disk has enough space available, Retrospect keeps a backup of each source for every day in the last week, a backup for each week in the last month, and a backup for each previous month.

WARNING: Grooming deletes files and folders. These files and folders cannot be recovered. Before enabling grooming, make sure you have a backup policy that protects your critical files and folders.

Recycling Options for Tape Drive Backups

If you are backing up to a tape drive, you can tell Retrospect to "recycle" the destination tape Backup Set before backing up to it. Recycling enables you to reuse the tapes in a Backup Set, however all data on those tapes is lost.

WARNING: Before recycling a tape Backup Set make sure the data on its tapes exists elsewhere or that you can really afford to lose the data.
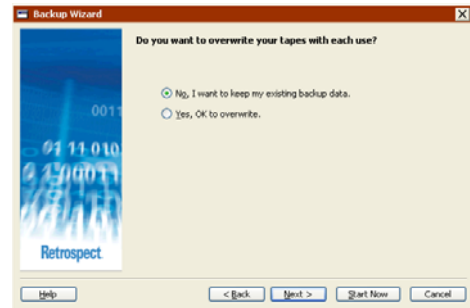
- **No, I want to keep my existing backup data**: Choose this option to preserve all existing backup data in the tape Backup Set. Retrospect backs up only new and changed files since the last backup to this Backup Set. If the current tape member fills up, Retrospect asks for a new tape.

- **Yes, OK to overwrite**: Choose this option to recycle the tape Backup Set before backing up. When Retrospect performs a recycle backup, it clears the Backup Set's Catalog File contents (if any), so it appears that no files are backed up. Then it looks for the first tape member in the Backup Set and erases it if it is available. If the first member is not available, Retrospect uses any available new or erased tape. All selected files are backed up.

TIP: In Advanced Mode, you can recycle a tape Backup Set by enabling the Recycle backup execution option.

Each time you start an immediate backup to a tape Backup Set, Retrospect asks if you want to recycle the Backup Set first.

MEDIA LONGEVITY AND STORAGE

Media life depends largely upon how the media is stored and maintained. Proper storage avoids moisture, heat, and particulate contamination, which cause media deterioration, leading to loss of media integrity or loss of data itself.

Magnetic media's worst enemy is moisture. Optical media's worst enemy is heat, which causes distortion, and particulate matter, which causes scratches. Keep media out of direct sunlight and away from heaters. Avoid extreme temperature changes. Airborne particulates such as dust and cigarette smoke can also harm media.

Tapes are unique in that they use lubricant. The tape media is lubricated, and after many passes over the drive's heads, tapes tend to fail because the lubricant has dissipated. You should be able to get a few thousand passes from a tape, but remember that each tape operation involves several passes.

A fire-proof safe in a climate-controlled building is an ideal media storage location. At the very least, keep the media in its original containers inside a cabinet or desk.

MULTIPLE BACKUP DRIVES

During an operation, Retrospect searches available backup devices for the appropriate medium. If the medium fills or Retrospect needs another medium for any reason, it searches available drives. Thus, you can have one drive with the tape Retrospect expects and another drive with an empty tape for when the first tape fills during the night. The drives must use similar mechanisms, such as two Travan drives.

With Advanced Tape Support add-on, Retrospect can work with multiple drives simultaneously. If you have two tape drives, or a tape library with multiple drives, Retrospect can back up data to both drives concurrently

(provided the backups have unique sources). See "Multiple Concurrent Executions" on page 161 for more information.

NETWORK ATTACHED STORAGE (NAS) DEVICES

Retrospect works with Network Attached Storage (NAS) devices in a number of ways. You can run the Retrospect application or Retrospect Client on the NAS device, or you can use the NAS device as the destination to store data for disk Backup Sets.

Backing up to a NAS Device

Retrospect works with a NAS device the same way it works with any other network volume. If you can access the device from Windows Explorer, Retrospect can use it as a destination.

To use a NAS device as a backup storage destination, create a disk Backup Set and select the NAS volume as its media.

Backing up a Windows-based NAS Device

If you are storing a lot of data on a NAS device, it's important to back it up. You can back up a NAS device as a network volume (see "Microsoft Networking Volumes" on page 197), although that is not the best method.

Tqzkq recommends that you install the Retrospect application or Retrospect Client on the NAS device, then back it up locally or remotely using Retrospect.

In order to run the Retrospect application, the NAS device requires:

• Windows 2000 Server or later with Microsoft Server Appliance Kit; or Windows Storage Server 2003

• Retrospect Single Server or Retrospect Multi Server

NOTE: *All* of the Wizard Mode options are available in Advanced Mode. If you switch from Wizard to Advanced Mode, those options are mapped directly to equivalent options.

Backing Up in Advanced Mode

Backing up in Advanced Mode provides access to some powerful Retrospect options that are not available in Wizard Mode. In Advanced Mode you can:

- Access more built-in selectors
- Create and apply custom selectors
- Preview and select specific files to back up
- Set many additional options not available in Wizard Mode

To set up an Immediate Backup in Advanced Mode, click Backup from the navigation bar, then click the Backup button.

If the Backup Wizard welcome screen displays, click Switch to Advanced Mode. The Immediate Backup summary window displays.
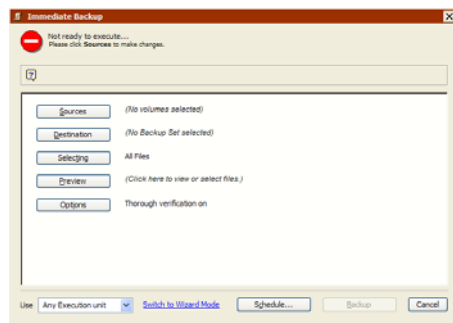
Click the buttons on the summary screen to specify the source, destination, and other backup options.

Choosing Source Volumes

In the Immediate Backup summary window, click the Sources button to display the Source Selection window.
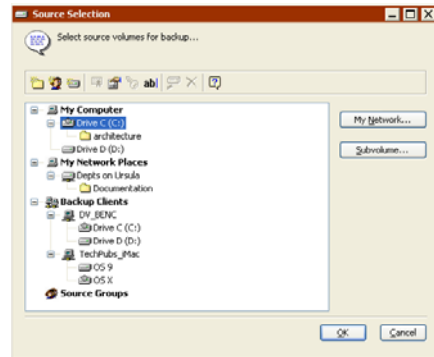
It lists all volumes currently available to be backed up, including your internal hard disk, any mounted removable disks or hard disks, any logged-in client volumes, and any connected network volumes from file servers.

NOTE: If you have the SQL Server Agent and/or Exchange Agent add-on, SQL and/or Exchange servers and mailboxes are also listed. See Appendix A: SQL Server Agent and Appendix B: Exchange Server Agent for more information.

In the volume list, click a volume to select it. To back up more than one volume, Shift-click or Control-click other volumes.

When you have made your source selection, click OK to continue setting up the immediate backup. The source selection window closes and Retrospect returns to the Immediate Backup window.

Choosing the Backup Set

In the Immediate Backup summary window, click the Destination button to display the Backup Set selection window, which lists available Backup Sets.
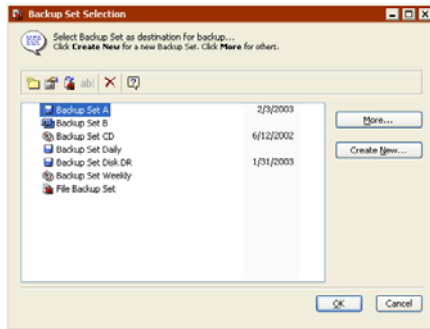
Select the destination Backup Set and click OK to continue setting up the backup. If no Backup Sets are listed in the Backup Set selection window, or if you do not wish to use any of those listed, click Create New to create a new Backup Set. See "Creating Backup Sets" on page 252 for more information.

Setting Additional Options

After you have specified the source volume to back up and the destination Backup Set to which it will be copied, use the Immediate Backup summary window to verify your choices and set additional options.

To makes changes, click the appropriate button.

Sources lets you add or remove source volumes.

Destination lets you choose a different Backup Set as a destination.

Selecting lets you choose a selector, a kind of filter for selecting files and folders to be backed up. (Selectors are explained in detail in "Using Selectors" on page 291.) The default selector is "All Files Except Cache Files" which marks all files (except cache files) on the source for backup.

Preview scans the source volume (or volumes) and determines which files need to be backed up by comparing the source files against the list of files in the Backup Set Catalog. When the scan is complete, Retrospect opens a browser window to display a list of the files on the source volume marked for backup. You can use it to mark and unmark individual files and folders to be backed up.

Browsers are explained in "Browsing" on page 286. When you close the browser, the summary window shows figures for the selected files.

Options displays the basic options window in which you can specify the backup action (Normal or Recycle), choose a verification method, and turn software data compression on or off.
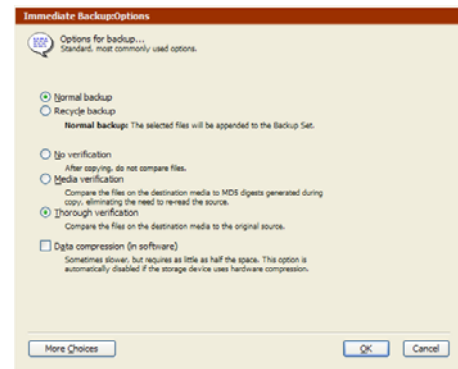
Click the More Choices button to access many more options.

Backup actions are explained in "Backup Actions" on page 24, and options are explained in detail under "Backup Execution Options" on page 237.

Executing the Backup

If Retrospect has the information it needs, it says "Ready to Execute" at the top of the Immediate Backup summary window. If the information is incomplete, it says "Not Ready to Execute" and you must change one or more parts of the information, as described at the top of the window.

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this operation (or choose "Any Execution unit'). Make your selection in the summary window's combo box. See "Assigning Execution Units" on page 162 for more information.

When you are ready, click Backup. Retrospect scans the source volume, then displays the Activity Monitor window.

Monitoring the Backup

The Activity Monitor displays the progress of the operation and the names of files as they are copied to the destination Backup Set. The Activity Monitor window also has Pause and Stop buttons for suspending or cancelling the backup.
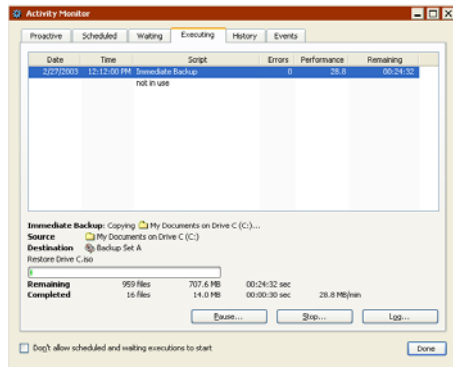
If the destination Backup Set does not have any members, or if the backup device does not have the correct media loaded, Retrospect displays a media request window. The window varies

slightly depending on the type of Backup Set you are using.
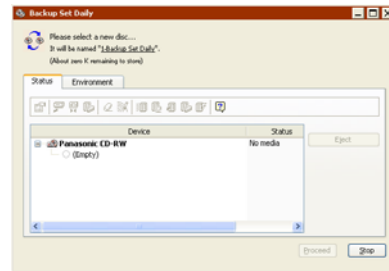
Insert a blank tape or CD/DVD, or one with unwanted data, because any files on it will be permanently removed. Select the new media in the window, then click Proceed.
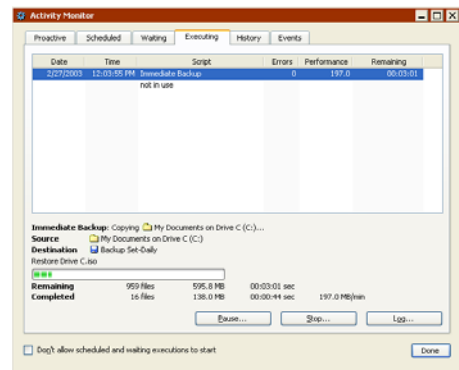
When the execution is complete, click the History tab to see performance data for the backup. If any errors occurred you get more information by clicking the Errors button. To view the Operations Log for this execution, click the Log button.

This log is described in "Viewing the Operations Log" on page 231.

Editing the Backup Settings

Retrospect automatically remembers the most recent settings you specified for an immediate backup. To view and edit those settings choose Backup>Backup from the navigation bar.

TIP: If the Wizard Mode backup summary screen displays, click Switch to Advanced Mode.

To back up again with the same settings, click Backup

To edit the settings, click the buttons to change the sources, destination, file selection criteria, and options. Editing the settings in Advanced Mode is the same as creating them the first time. See "Backing Up in Advanced Mode" on page 61 for more information.

To edit the settings in Wizard Mode, click "Switch to Wizard Mode". See "Switching from Advanced to Wizard Mode" for more information.

Scripting the Backup

If you want to automate your backups so they can be performed while your computer is unattended (e.g., when you go home at night), you can use Retrospect's scripting feature to set up and schedule backups.

From the Immediate Backup summary window, click the Schedule button to save the immediate backup information and settings as a script. You can then add a schedule to the script to accomplish automatic, unattended backup operations.

See "Scheduling Scripts" on page 134.

Switching from Advanced to Wizard Mode

In general, Tqzkq recommends editing immediate backups in the same mode you created them. Of course, you can switch between the modes and if you do, it's important to know how Retrospect handles advanced options that are not available in Wizard Mode.

To return to Wizard Mode at any time, click "Switch to Wizard Mode" from the Advanced Mode summary window.

If you have made any changes to your backup settings, Retrospect asks if you want to save those changes before switching modes.
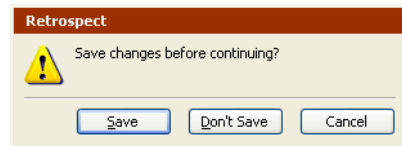
If you have not made any changes, Retrospect displays the Wizard Mode Welcome screen with a summary of the current backup settings.

Since Advanced Mode includes options not available in Wizard Mode, Retrospect must either keep those settings, or discard them. There are a few important options to consider:

- Selectors
- Execution Options
- Backup Sets
- Manual File Selection
- Execution Unit

Selectors

Advanced Mode includes a number of built-in selectors that are not available in Wizard Mode. In addition, you can create and use custom selectors in Advanced Mode.
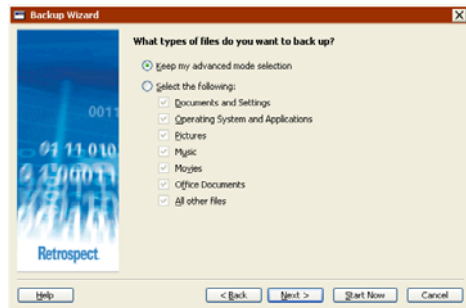
If you choose a selector that is not available in Wizard Mode, then click "Switch to Wizard

Mode", Retrospect *keeps* the advanced selector and applies it when you run the backup.

In these situations, the Wizard Mode Welcome screen displays *(Created in Advanced Mode)* in the Selecting field.

In addition, if you edit your backup settings, a new option appears in the "What type of files do you want to back up?" screen.

- Choose "Keep my advanced mode selection" to keep your advanced selector.
- Choose "Select the following" and select a new option to discard the advanced selector and use a new one.

Execution Options

Advanced Mode includes many execution options that are not available in Wizard Mode, such as verification and backup action.

NOTE: The compression execution option is available in both Wizard and Advanced Mode.

If you change the option in one mode, it will be reflected in the other.

If you choose an execution option that is not available in Wizard Mode, then click "Switch to Wizard Mode", Retrospect *keeps* the advanced execution option and applies it when you run the backup.

WARNING: The Wizard Mode Welcome screen does not indicate whether the backup includes advanced execution options or not. The only way to check is to switch to Advanced Mode and review the Options settings.

Backup Sets

In Advanced Mode, you can choose a file Backup Set as the destination. File Backup Sets are not available from Wizard Mode.

TIP: File Backup Sets are most useful for backing up a single file, otherwise, disk Backup Sets offer many more benefits.

If you choose a file Backup Set as the destination, then click "Switch to Wizard Mode", Retrospect *discards* the destination.

In these situations, the Wizard Mode Welcome screen displays *(No destination selected)* in the Destination field.

If you click Next, the wizard discards the destination and forces you to select a new one. Click "Switch to Advanced Mode" to continue using the file Backup Set as the destination.

Manual File Selection

In Advanced mode, you can click the Preview button and select specific files and folders to back up. If you do this, the Advanced Mode summary window displays *(Manual selection)* in the Selecting field.
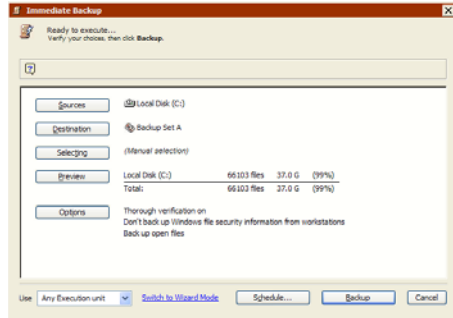
If you apply a manual selection, then click "Switch to Wizard Mode", Retrospect *discards* the selection. There is no way to perform manual selection in Wizard Mode.

Execution Unit

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for a backup operation in Advanced Mode only.

If you choose a specific execution unit (not "Any Execution unit"), then click "Switch to Wizard Mode", Retrospect *keeps* the execution unit information and uses the specific execution unit when you run the backup.

NOTE: The Wizard Mode Welcome screen does not indicate whether the backup specifies an execution unit or not. The only way to check is to switch to Advanced Mode and review the settings.

ARCHIVE

Archiving lets you copy files from a volume to a Backup Set for off-line storage. To set up an archive operation, first click Tools from the

navigation bar, then click Archive Files. The archive summary window displays.
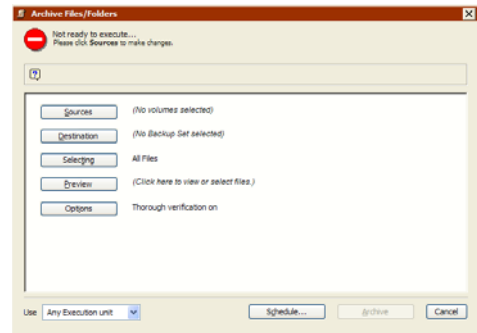
As with backups, there are three basic steps in archiving:

- Choosing the source volumes to archive
- Choosing the Backup Set in which to store the files (or creating a new Backup Set)
- Executing the archive

NOTE: Be sure to read "Archiving Tips" on page 68 for important information about archiving.

Choosing the Source Volumes

In the archive summary window, click the Sources button to display the Source Selection window.
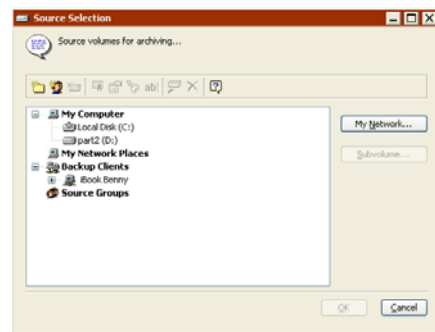
It lists all volumes currently available to be archived, including your internal hard disk, any mounted removable disks or hard disks, any

logged-in client volumes, and any connected network volumes from file servers.

NOTE: You cannot archive SQL or Exchange databases, nor can you archive Exchange mailboxes or Public Folders.

In the volume list, click a volume to select it. To archive more than one volume, Shift-click or Control-click other volumes.

When you have made your source selection, click OK to continue setting up the immediate archive. The Source Selection window closes and Retrospect returns to the archive summary window.

Choosing the Backup Set

In the archive summary window, click the Destination button to display the Backup Set selection window, which lists available Backup Sets.
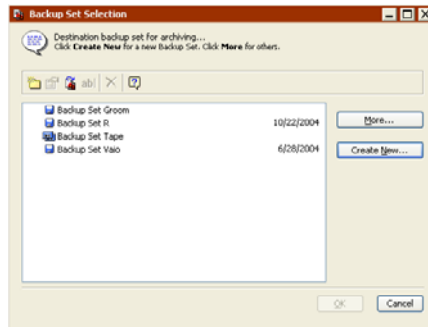
Select the destination Backup Set and click OK to continue setting up the archive. If no Backup Sets are listed in the Backup Set Selection window, or if you do not wish to use any of those listed, you can create a new Backup Set. See "Creating Backup Sets" on page 252 for more information.

WARNING: Do not archive files to a disk Backup Set that has grooming enabled. Since grooming deletes older Snapshots to make room on the disk for new ones, it defeats the purpose of creating a permanent archive.

Setting Additional Options

After you have specified the source volume to archive and the destination BackupSet to which it will be copied, use the archive summary window to verify your choices and set additional options.
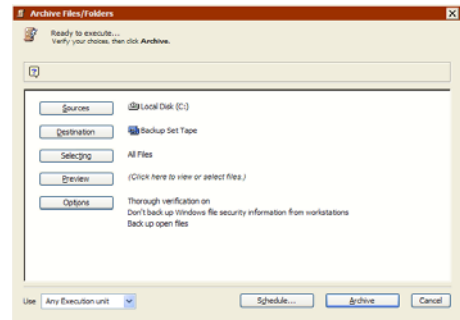
To makes changes, click the appropriate button.

Sources lets you add or remove source volumes.

Destination lets you choose a different Backup Set as a destination.

Selecting lets you choose a selector, a kind of filter for selecting files and folders to be archived. (Selectors are explained in detail in "Using Selectors" on page 291.) The default selector is "All Files" which marks all files on the source for archive.

Preview scans the source volume (or volumes) and opens a browser window to display a list of the files on the source volume. You can mark and unmark individual files and folders to be archived.

NOTE: Unlike backing up, archiving, by default, does not match source and destination. That is, Retrospect does not compare source files to files in the destination Backup Set. Therefore, it is possible that Retrospect will copy files that already exist in the destination Backup Set. In this case, Retrospect is

foregoing ultimate efficiency for the sake of archive integrity.

Browsers are explained in "Browsing" on page 286. When you close the browser, the summary window shows figures for the selected files.

Options displays the basic options window in which you can set the verification, software data compression, and move files options.
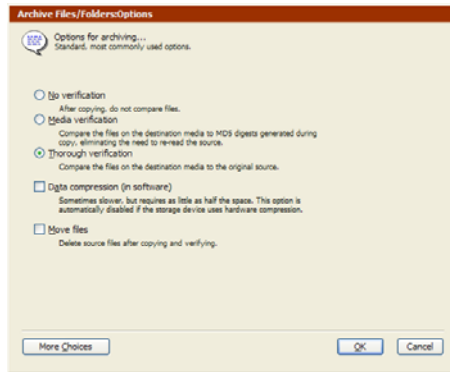
If you enable the "Move files" option, Retrospect deletes the original files from the source after copying them to the destination and verifying that they were copied correctly. This frees space on the volume.

TIP: Before you use the Move files option, first archive to a different Backup Set by copying without moving. This provides an extra measure of safety should one Backup Set become unusable.

The verification and software data compression options are explained in detail in "Backup Execution Options" on page 237.

Click the More Choices button to access many more options. See "Execution Options" on page 236 for more information about these options.

NOTE: See "Archiving Tips" on page 68 for more information about using archiving options.

Executing the Archive

If Retrospect has the information it needs, it says "Ready to Execute" at the top of the archive summary window. If the information is incomplete, it says "Not Ready to Execute" and you must change one or more parts of the information, as described at the top of the window.

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this operation (or choose "Any Execution unit'). Make your selection in the summary window's combo box. See "Assigning Execution Units" on page 162 for more information.

When you are ready, click Archive. Retrospect scans the source volume, then displays the Activity Monitor window.

At this point, the archive operation is just like a backup operation. See "Executing the Backup" on page 63 for more information.

Scripting an Archive

When an archive summary window is active, you can click the Schedule button to save the archive information and settings as a script.

See Chapter 5 • Automated Operations.

Archiving Tips

Media: Plan for the long term. Archive to two or more Backup Sets and maintain an off-site copy of your archived data. Always store media according to manufacturer's guidelines. See "Media Longevity and Storage" on page 50 for further information.

Periodically transfer your data to new media to ensure storage integrity. Do not use device-specific options such as hardware compression, because your next backup device may not support features of an older model.

Planning: Define an archiving system and follow it every time. Only archive files in specific

folders, or modified within a specific date range. Force users to make a decision on what is to be archived by moving data to a specific location. Never archive data without telling users what was removed.

Before you use the Move files (delete after copy) option, first archive to a different Backup Set by copying without moving. This provides an extra measure of safety should one Backup Set become unusable. If you have only a single archive medium and it is lost or damaged, you will have lost all of your data. Be sure not to recycle, groom, lose, or damage your archive media.

Verification: Always use verification. If you do not use verification and hardware problems occur when archiving, your data may not be correctly copied to the media. When archiving with the "Move files" option on, you should use Thorough verification (*not* Media verification).

On-line Archiving: To archive documents in place, compress them in a disk Backup Set that you store on your hard disk. This way they take up less room, but are still on-line.

Grooming: Do not archive files to a Backup Set that has grooming enabled. Since grooming deletes older Snapshots to make room on the disk for new ones, it defeats the purpose of creating a permanent archive.

RESTORE

Retrospect allows you to restore an entire volume or restore selected files and folders from the most recent backup or any previous backup. Retrospect can restore selected files and folders, entire volumes, or just the System State and registry. You can restore either by selecting a Snapshot from a Backup Set, or by searching through one or more Backup Sets for files that meet specified criteria. This section focuses on

those two methods of restoring files with Retrospect.

If you have experienced disastrous data loss in which the computing environment required to restore data is not available, see Chapter 8 • Disaster Recovery, which includes an overview of different situations and points you to restore instructions.

NOTE: To restore files that were backed up with Open File Backup, make sure to close or stop the application that uses the open files on the destination volume.

For information on how to restore a SQL database, or an Exchange mailbox or database, see Appendix A: SQL Server Agent and Appendix B: Exchange Server Agent.

If you have the User Initiated Restore add-on, supported Retrospect Client users can restore their own files from recent hard disk backups without requiring administrator intervention. See "User Initiated Restore" on page 191 for more information.

Snapshots

Retrospect's Snapshots make it easy to restore an entire volume or a selected file to its exact state as of a given date and time. A Snapshot is like a picture of the contents of a volume at a point in time. It contains a list of all of the files and folders on a volume and the sessions during which they were backed up. Each time you back up a volume, its Snapshot is updated in the Backup Set Catalog and the Snapshot is added to the backup medium.

To restore an entire volume, simply choose the Snapshot you want to restore and Retrospect will automatically locate and retrieve the necessary files, even if they were backed up in different sessions. A Snapshot allows Retrospect to restore the files from a Backup Set in a single pass through the media, rather than hav-

ing to restore each incremental session individually and in a specific order.

You can also restore individual files from a Snapshot. This is the easiest way to retrieve files that you know were on a volume at a specific time. If you are not sure which Snapshot or even which Backup Set contains the files you want to retrieve, you can define search criteria to help find the files. See "Restoring by Search" on page 78 for more information.

You can restore by Snapshot in either Wizard Mode or Advanced Mode.

Restoring In Wizard Mode

The Restore Wizard provides an easy way to set up and edit immediate restore operations. To start the Restore Wizard, click Restore from the navigation bar, then click the Restore button.

The Restore Wizard welcome screen displays.

Welcome Screen

When you choose Restore>Restore from the navigation bar, Retrospect always opens the Restore Wizard. Click Next to continue set up using the Restore Wizard.
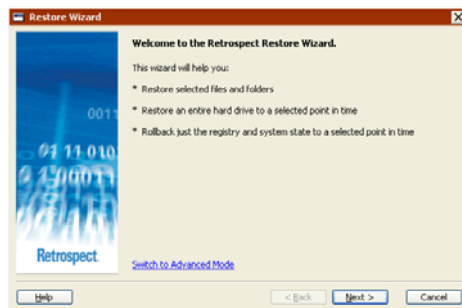
To set up the restore in Advanced Mode, click Switch to Advanced Mode. See "Restoring in Advanced Mode" on page 73 for more information.

Selecting a Backup Set

Select the Backup Set that contains the files you want to restore and click Next.

The Backup Set list displays all current Backup Sets by name and includes information on when each Backup Set was last modified. The icons next to the Backup Set names indicate the Backup Set type (e.g., disk, tape, etc.).

If the Backup Set containing your files is not displayed, click More Backup Sets, browse to the location of the Backup Set's Catalog File (by default, ..My Documents\Retrospect Catalog Files), select a Backup Set, and click Open.

If you cannot find the Backup Set's Catalog File, click Recreate to recreate it from the backup media. See "Recreating a Catalog" on page 302 or "Repairing a File Backup Set" on page 304 for more information.

Selecting a Snapshot

Select the Snapshot that contains the files you want to restore and click Next.
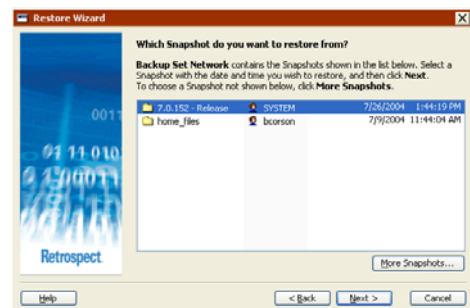
The Snapshot list displays all the *active* Snapshots for the selected Backup Set by name and includes information on the date and time each Snapshot was made. The icons next to the Snapshot names indicate what was backed up (e.g., a drive, a folder, etc.).

If the Snapshot you want to use is not listed, click the More Snapshots button to display a list of *all* Snapshots in the Backup Set.

TIP: To restore files from a backup other than the most recent one you will most likely need to click More Snapshots.

In the Snapshot Retrieval window, select a Snapshot and click Retrieve. Since Retrospect retrieves older Snapshots from the Backup Set media, you may be required to insert the media into your backup drive.

NOTE: The Retrieve button is disabled when you select a Snapshot that is already available.

Choosing the Destination

You can restore files either to their original location or to a new location.
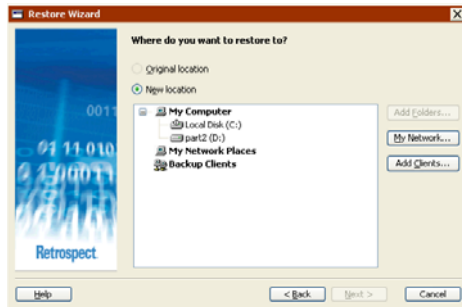
NOTE: The Original location option is only available if the location still exists and is accessible to Retrospect.

To restore to a new location, choose New location, then specify a destination. Click a drive or folder to select it. This deselects any other selected drive or folder. You can select a drive or folder from any of the containers listed in this screen: My Computer, My Network Places, or Backup Clients.

• To add Retrospect Clients to the Backup Clients container, click Add Clients.

• To add network volumes to the My Network Places container, click My Network.

• To display the folders on a drive, select the drive and click Add Folders.

NOTE: The My Network button and My Network Places container are not displayed if your Snapshot contains a full system backup.

Choosing the Type of Restore

Depending on the selections you made earlier in the wizard, this screen offers some combination of the following options:

• **Restore files and folders** allows you to select specific files to restore to the destination.

• **Restore everything...deleting all other contents** deletes all the existing files on the destination, then restores all the files in the Snapshot to the destination.

• **Rollback everything...** deletes all the existing files on the destination, then restores all the files in the Snapshot to the destination. This option also restores the registry and System State information from the source Snapshot.

• **Rollback just the registry and system state** does not restore any files from the Snapshot or delete any files from the destination. This option restores *only* the registry and System State information from the source Snapshot.

Select an option and click Next.

Selecting the Files to Restore

This screen offers different options depending on the selection you made in the previous screen of the wizard.

If you chose "Restore files and folders", click Select Files to display a list of the files available to restore from the Snapshot. Select the check box next to each file you want to restore (by default, all files are selected). Selecting the check box for a folder selects all files in that folder.

If you chose "Restore everything..." or "Rollback everything...", Retrospect selects *all* files. Click Preview Files to display a list of the files that will be restored from the Snapshot. Clear the check box next to files that you do *not* want to restore. Clearing the check box for a folder clears the check boxes for all files in that folder.

Setting the Matching Option

When the restore destination already contains files you selected to restore, you can choose to replace those "matching" files with the ones from the source Backup Set's Snapshot.

• **Never** matching files on the destination are left untouched. This option restores all selected files from the Snapshot that do not exist on the destination, but does not overwrite any files on the destination. It is useful if you want to make sure you don't restore an older version of a file you have updated since the Snapshot was taken.

• **Only if Backup Set is newer**, matching files on the destination are replaced by the selected files from the Snapshot *only* if the Snapshot files are newer. This option restores all selected files from the Snapshot that do not exist on the destination and overwrites matching files on the destination if Snapshot file is newer than the destination file.

• **Always**, matching files on the destination are *always* replaced by the selected files from the Snapshot. This option restores all selected files from the Snapshot that do not exist on the destination and overwrites matching files on the destination. The Always option replaces matching

destination files with files from the Snapshot regardless of whether the Snapshot file is newer or older than the destination file. This option is most useful if you want to restore an older version of a file that has been corrupted since the Snapshot was taken.

Reviewing the Restore Settings

The Restore Summary screen displays the restore settings you specified in the wizard.
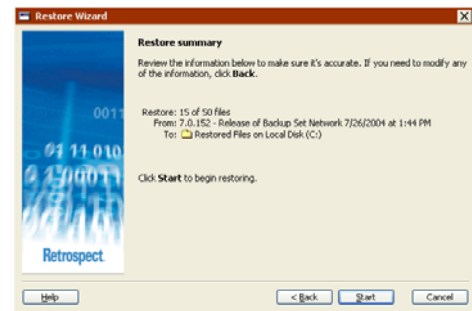
• **Restore** lists the number of files that will be restored

• **From** lists the volume name and date and time of the Snapshot, as well as the name of the Backup Set that contains the Snapshot. If the Backup Set is stored on removable media, make sure it is loaded in your backup device.

• **To** lists the destination to which data will be restored.

NOTE: Some options specified in the wizard are not listed in the summary screen (e.g., matching and type of restore), but they are implemented during the restore.

To change any of the restore settings, click Back.

To start the restore, click Start.

Monitoring the Restore

This screen includes information on the restore destination and information about the progress of the restore operation.
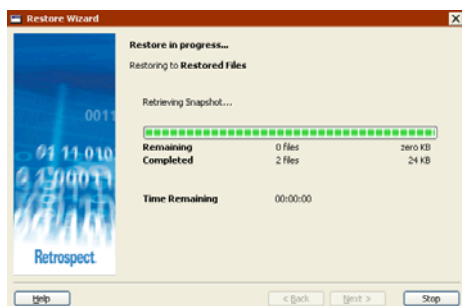
- **Remaining** lists the number of files that need to be restored and their combined size.
- **Completed** lists the number of files already restored and their combined size.
- **Time Remaining** provides an estimate of the time remaining until the restore is complete.

Click Stop to halt the restore operation. Click Yes in the confirmation dialog to stop the operation and exit the wizard.

NOTE: Retrospect's Activity Monitor runs in the background and includes more information about the restore operation. See "Activity Monitor" on page 152 for more information.

Successful Restores

If Retrospect restores the selected files without encountering any errors, it displays the Congratulations screen. Browse to the destination to see the restored files.

Click Close to exit the wizard.

NOTE: If you performed a system restore (i.e. "rollback") you must reboot the destination computer.

Restores with Errors

If Retrospect encounters errors during the restore, it displays a warning screen.

Click Open Log to display the Operations Log for the restore operation. The log includes information on the errors Retrospect encountered, as well as information about the number of files (if any) that were successfully restored before the errors.

Click Cancel to exit the wizard.

Restoring in Advanced Mode

Advanced Mode immediate restores include all of the options available in Wizard Mode, plus a few additional options not available in the wizard. In Advanced Mode you can:

- Save your restore settings as a script
- Restore using the "Retrieve Just Files" method
- Specify an execution unit to use for the restore operation (if your version of Retrospect supports multiple execution units)
- Set some additional options not available in Wizard Mode (e.g. update modify dates)

In general, you should restore using whichever mode is more comfortable for you, unless you need to use Advanced Mode options not available in Wizard Mode.

To restore in Advanced Mode, click Restore from the navigation bar, then click the Restore button. The Restore Wizard welcome screen displays.

Click Switch to Advanced Mode.

NOTE: To restore in Wizard Mode, see "Restoring In Wizard Mode" on page 70
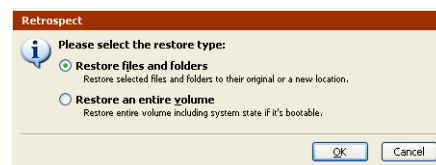

Choose the type of restore:

- **Restore files and folders**, allows you to select specific files and folders to restore to

a new folder on the destination, leaving the rest of the destination unchanged.

- **Restore an entire volume**, selects and restores all files and folders from the source Snapshot to the destination, deleting all other contents. Restores registry and System State information from the Snapshot (if available).
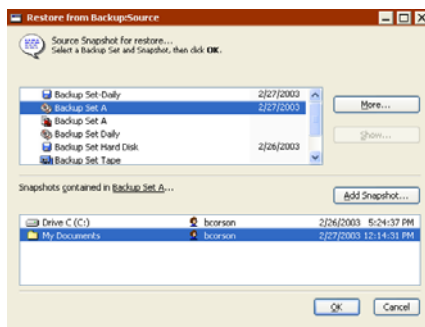
NOTE: The descriptions above describe the default behavior for the restore types. This behavior can be modified later by changing the defaults.

The Immediate Restore summary window displays.
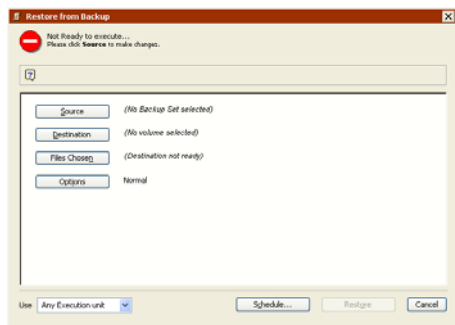
Click the buttons on the summary screen to specify the source, destination, and other restore options.

Selecting the Source

In the source selection window's top list, select the Backup Set from which to restore. You can use the More button if your desired Backup Set is not listed.

In the window's bottom list, select a volume Snapshot. The date and time of the Snapshot are listed to the right of the volume's name. If the Snapshot you want to use is not listed, click the Add Snapshot button to display a list of all Snapshots in the Backup Set.

TIP: To restore files from a backup other than the most recent one you will most likely need to use Add Snapshot.
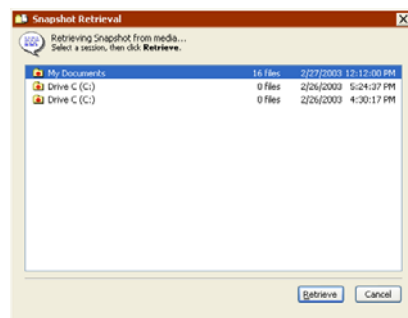
When you select a Snapshot and click Retrieve Retrospect obtains the older Snapshot from the Backup Set media (which may require you to insert media) and adds it to the list in the restore source window.

NOTE: The Retrieve button is disabled when you select a Snapshot that is already available.

With your desired Snapshot selected in the source selection window, click OK.

Selecting the Destination
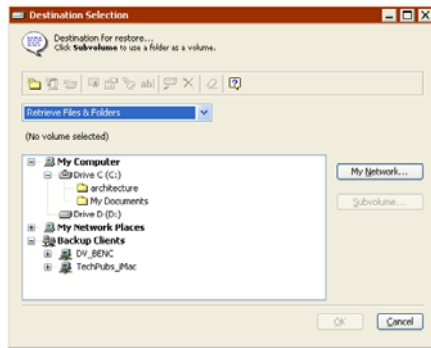
Select a volume on which you want Retrospect to place the restored files. This volume does not have to be the original volume from which the files were backed up; it can be a folder defined as a Subvolume (see "Subvolumes" on page 284) or any available volume, including one belonging to a client on the network. (Navigate through My Computer, My Network Places, and Backup Clients as detailed in "Containers" on page 281.)

Choosing the Method to Restore Files

Set the list box to determine how Retrospect restores the files to the destination.

Restore Entire Volume makes the destination volume exactly match the source Snapshot. It *deletes all files and folders* on the destination that do not match those marked for restore in the Snapshot, leaving files untouched if they are identical to files marked for restore. It then copies all remaining files and folders from the Snapshot to the destination, preserving the folder hierarchy. This is the default restore method if you chose "Restore an entire volume". If you select this method, Retrospect restores registry and System State information from the Snapshot (if both the Snapshot and destination are system volumes) by default.

NOTE: To prevent the operating system from crashing, the Restore Entire Volume method does not delete the active Windows system, nor does it delete the "blessed" system folder of a Mac OS client.

Replace Corresponding Files restores all selected files from the Snapshot that do not exist on the destination and overwrites files on the destination that also exist in the source Snapshot. These "corresponding" or "matching" files on the destination are *always* overwritten with files from the Snapshot regardless of whether the Snapshot file is newer or older than the destination file. Retrospect leaves files untouched if they are identical to files marked for restore, if the file names do not match those marked for restore, or if the path to those files is not identical. If you select this method and choose the Restore System State execution option, Retrospect restores registry and System State information from the Snapshot (if both the Snapshot and destination are system volumes).

Replace if Backup is Newer restores all selected files from the Snapshot that do not exist on the destination and overwrites matching files on the destination only if the Snapshot file is newer than the destination file. If you select this method and choose the Restore System State execution option, Retrospect restores registry and System State information from the Snapshot (if both the Snapshot and destination are system volumes).

Restore Missing Files Only restores all selected files from the Snapshot that do not exist on the destination, but does not overwrite any files on the destination. Matching files on the destination are left untouched. If you select this method and choose the Restore System State execution option, Retrospect restores registry and System State information from the Snapshot (if both the Snapshot and destination are system volumes).

TIP: To restore *just* the registry and System State, choose "Restore Missing Files Only", then click Files Chosen and make sure no files are selected, and finally click Options>More Choices and select the Restore System State check box.

Retrieve Files & Folders creates a new folder on the destination volume (giving the folder the name of the Backup Set), then copies all selected files from the Snapshot into this folder, preserving the Snapshot folder hierarchy. Nothing is replaced or overwritten. This is the default restore method if you chose "Restore files and folders". This method never restores registry and System State information.

Retrieve Just Files creates a new folder on the destination volume (giving the folder the name of the Backup Set), then copies all selected files from the Snapshot into this folder. The Snapshot folder hierarchy is *not* preserved. Nothing is replaced or overwritten. This method never restores registry and System State information.

The following table summarizes the restore methods:

Restore Method	Files in the Snapshot but not on the destination	Files in both the Snapshot and destination	Files on the destination but not in the Snapshot
Restore Entire Volume	Restored	Always overwrites the destination files	Deleted
Replace Corresponding Files	Restored	Always overwrites the destination files	Left untouched
Replace if Backup is Newer	Restored	Overwrites destination files if Snapshot files are newer	Left untouched
Restore Missing Files Only	Restored	Never overwrites destination files	Left untouched
Restore Files & Folders	Restored to a new folder	Never overwrites destination files	Left untouched
Restore Just Files	Restored to a new folder	Never overwrites destination files	Left untouched

After setting the destination restore method with the list box, click OK to continue. Depending on the restore type and method, Retrospect may scan the destination volume and match files from the selected Snapshot. Then the restore summary window appears.

Summarizing the Restore Operation
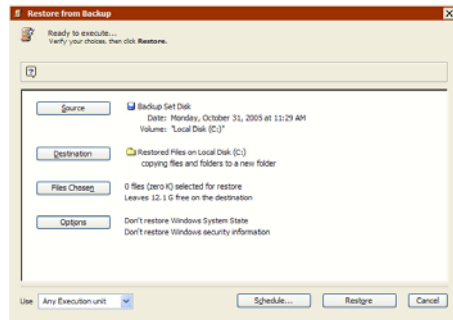
Verify your choices for the Source, Destination, Files Chosen, and Options. To change information, click the appropriate button.

Source is the Backup Set and volume Snapshot from which you want to restore files. Click this button to use the source selection window to change the source.

Destination is the volume to which you want to restore files. Click to change the destination volume or restore method.

Files Chosen are the files you want to restore from the Backup Set. If you chose "Restore entire volume", all files from the source Snapshot are selected by default. If you chose "Restore files and folders", no files are selected by default. Click this button to use a browser to mark and unmark individual files and folders to be restored. Browsers are explained in detail in "Browsing" on page 286.

Options let you set various execution options, including restoring the System State and updating the modification dates of restored files. Click this button, then click More Choices to set

these options. See "Execution Options," which starts on page 236, for more information.

Executing the Restore

When Retrospect has the information it needs to do the restore, it says "Ready to Execute" at the top of the restore summary window. If the information is incomplete, it says "Not Ready to Execute" and you must change one or more parts of the information you gave it.

WARNING: Restoring can destroy data on the destination. Make sure you chose the correct restore method.

Make sure the correct Backup Set media is in the backup device. If Retrospect cannot access the required media, it asks you for it.

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this operation (or choose "Any Execution unit"). Make your selection in the summary window's combo box. See "Assigning Execution Units" on page 162 for more information.

When you are ready, click Restore. Retrospect displays the Activity Monitor window.

Monitoring the Restore

Retrospect performs the restore, displaying the progress of the operation in the Activity Monitor's Executing tab and listing the names of files as they are copied from the Backup Set media to the destination. The Activity Monitor window also has Pause and Stop buttons for suspending or cancelling the restore.
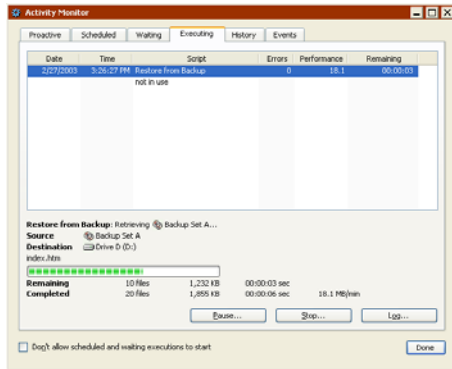
When the execution is complete, click the History tab to see performance data for the restore operation. If any errors occurred you can get more information by clicking the Errors button. To view the Operations Log for this execution, click the Log button.

This log is described in "Viewing the Operations Log" on page 231.

When you leave Retrospect and go to the destination volume, you can see that it is changed to reflect the restored files. The level of change can be anywhere from a new folder on the volume or a completely restructured volume from an entire volume restore, depending on the destination restore method and options.

NOTE: A Mac OS client's Desktop needs to be updated after a large restore, such as an entire volume. Restart the Macintosh while holding down the Command and Option keys to rebuild the Desktop.

Scripting the Restore

When a restore summary window is active, you can click the Schedule button to save the immediate restore information and settings as a script. You can then use the script to accomplish restore operations.

See Chapter 5 • Automated Operations.

Restoring by Search

While restoring by Snapshot lets you restore files from a specific backup date and time, restoring by search lets you retrieve one or more files regardless of when they were backed up. Restoring by search lets you search multiple Backup Sets at once, which is useful if you're not sure which Backup Set contains the files you want to restore. Searching works best when you know specific attributes of the files you want, for example it's name or type. If you want to see all backed up versions of a particular file, search on its name, and then restore exactly the version you want.

NOTE: Restore by searching does not restore NTFS permissions, AppleShare or Mac OS file sharing privileges, or registry and System State information. You must restore from a Snapshot to restore these.

To begin setting up a restore by search, click Restore, from the navigation bar, then click Find Files. The Backup Set Selection window displays.

Selecting the Backup Set(s) to Search
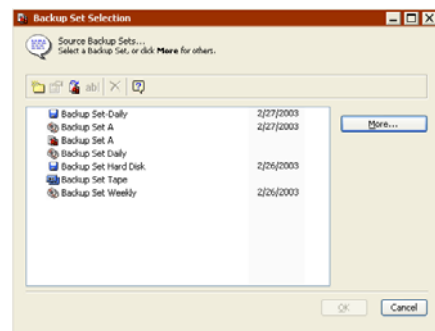
Select one or more Backup Sets to search. Click the More button if your desired Backup Set is not listed. Click OK to continue. The Destination Selection window displays.

Selecting the Destination
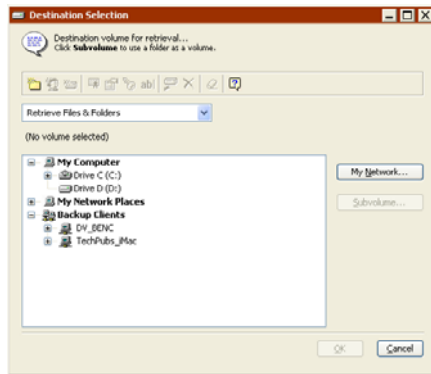
Select a volume on which you want Retrospect to place the restored files. This volume does not have to be the original volume from which the files were backed up; it can be a folder defined as a Subvolume (see "Subvolumes" on page 284) or any available volume, including one belonging to a client on the network. (Navigate through My Computer, My Network Places, and Backup Clients as detailed in "Containers" on page 281.)

Choosing the Restore Method

Set the list box to determine how Retrospect restores the files to the destination. The default setting is "Retrieve Files & Folders".

Restore Entire Volume replaces the destination volume with the selected files from the source Backup Set(s) that meet your search criteria. It *deletes all files and folders* on the destination that do not match those marked for restore in the Snapshot, leaving files untouched if they are identical to files marked for restore. It then copies all remaining files and folders from the Snapshot to the destination, preserving the folder hierarchy.

NOTE: To prevent the operating system from crashing, the Restore Entire Volume method does not delete the active Windows system, nor does it delete the "blessed" system folder of a Mac OS client.

Replace Corresponding Files restores all selected files from the source Backup Set(s) that meet your search criteria and do not exist on the destination. Files that exist on the destination that are also in the source Backup Set(s) and meet your search criteria are *always* overwritten. Retrospect leaves files untouched if they are identical to files marked for restore, if the file names do not match those marked for restore, or if the path to those files is not identical.

Replace if Backup is Newer restores all selected files from the source Backup Set(s) that meet your search criteria and do not exist on the destination. Files that exist on the destination that are also in the source Backup Set(s) and meet your search criteria are overwritten only if the Backup Set files are *newer*.

Restore Missing Files Only restores all selected files from the source Backup Set(s) that meet your search criteria and do not exist on the destination. Files that exist on the destination that are also in the source Backup Set(s) and meet your search criteria are *never* overwritten only.

Retrieve Files & Folders creates a new folder on the destination volume (giving the folder the name of the Backup Set), then copies all selected files from the source Backup Set(s) that meet your search criteria into this folder, preserving the Snapshot folder hierarchy. Nothing is replaced or overwritten.

Retrieve Just Files creates a new folder on the destination volume (giving the folder the name of the Backup Set), then copies all selected files from the source Backup Set(s) that meet your search criteria into this folder. The Snapshot folder hierarchy is *not* preserved. Nothing is replaced or overwritten.

After setting the restore method with the combo box click OK. Retrospect displays the searching and retrieval window.

Specifying the Search Criteria
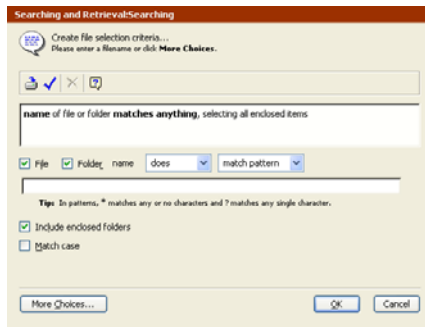
If you want to restore all files from all sources, click OK.

Otherwise, use the controls and enter text to define the search criteria on file or folder names, or click More Choices to make a custom selector with other search criteria. This window is described in detail in "Finding Files" on page 289, and selectors are described in "Using Selectors" on page 291.

When you have defined the search criteria, click OK. Retrospect searches each source Backup Set before displaying up the summary window.
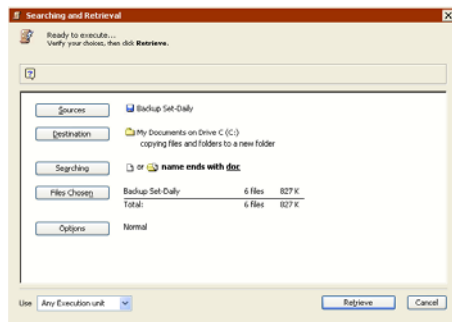
Your file selection criteria are summarized next to Searching. Files Chosen displays the total number of files from each source Backup Set that meet the search criteria.

Choosing Files to Restore

Click Files Chosen to open a browser that lists files meeting the search criteria. You can man-

ually unmark and mark these files for restore. See "Marking Files and Folders" on page 288 for more information. Files with check marks will be restored when the operation is executed.

TIP: Depending on your search criteria, your browser may list more than one version of a particular file. For example, a given file may have been modified daily and backed up every day over a certain period of time. Use the backed up or modified dates to determine which version you want to restore.

Modifying Search Criteria

If the browser does not display the files you want, you can close it and return to the summary window to redefine the search criteria by clicking the Searching button. If you change the search criteria, Retrospect displays a dialog asking whether you want to do a new search, narrow the existing search, or widen the existing search.
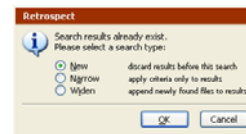
New replaces the results of the previous search with the results of the new search.

Narrow uses the new criteria to further restrict the selection.

Widen uses the new criteria to add files to the current selection.

Select a search type, then click OK to return to the summary window and repeat the process until you are satisfied with the chosen files.

Executing the Restore

If Retrospect has the information it needs, it says "Ready to Execute" at the top of the searching and retrieval summary window. If the information is incomplete, it says "Not Ready to

Execute" and you must change one or more parts of the information you gave it.

WARNING: Restoring can destroy data on the destination. Make sure you chose the correct restore method.

Make sure the correct Backup Set media is in the backup device. If Retrospect does not see the media it asks you for it in a window.

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this operation (or choose "Any Execution unit'). Make your selection in the summary window'scombo box. See "Assigning Execution Units" on page 162 for more information.

When you are ready, click Retrieve.

Monitoring the Restore

Retrospect performs the restore, displaying the progress of the operation in the Activity Monitor window, which includes buttons to pause or stop its execution.
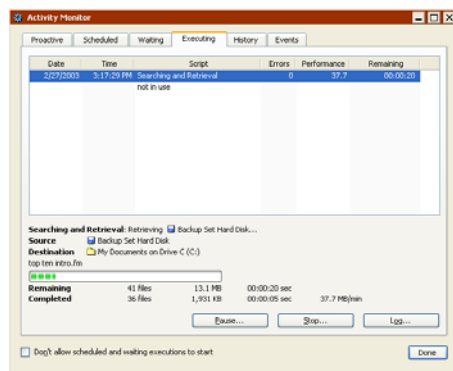
When the execution is complete, click the History tab to see performance data for the restore operation. If any errors occurred you get more information by clicking the Errors button. To view the Operations Log for this execution, click the Log button.

This log is described in "Viewing the Operations Log" on page 231.

When you leave Retrospect and go to the destination volume you can see it is changed to reflect the restored files.

NOTE: A Mac OS client's Desktop needs to be updated after a large restore. Restart the Macintosh while holding down the Command and Option keys to rebuild the Desktop.

DUPLICATE

An immediate duplicate copies selected files in their native file format from one drive or folder to another. After a duplicate operation, the destination drive contains an exact copy of every file and folder that was duplicated. You can open, edit, and otherwise work with the files.

NOTE: Files and folders are copied without compression and encrypted files remain encrypted.

Retrospect allows you to duplicate files from one drive to another, or duplicate files on the same drive from one folder to another. Retrospect optimizes the duplication process by copying only those files that do notalready exist on the destination.

There are two ways to set up an immediate duplicate. You can use Retrospect's Duplicate Wizard, which walks you throughthe process of setting up a duplicate, or you can set up the duplicate on your own in Advanced Mode. Advanced Mode has options that are unavailable in the Wizard. For more information see:

- Duplicating in Wizard Mode
- Switching from Wizard to Advanced Mode
- Duplicating in Advanced Mode
- Switching from Advanced to Wizard Mode

Duplicating in Wizard Mode

The Duplicate Wizard provides an easy way to set up and edit immediate duplicate operations. To start the Duplicate Wizard, click Backup from the navigation bar, then click the Duplicate button.

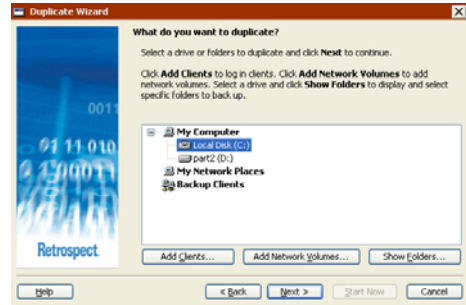**TIP:** If the Advanced Mode Duplicate Summary screen displays, click Switch to Wizard Mode.

Welcome Screen

If this is the first time you are setting up a duplicate, click Next to continue using the Duplicate Wizard. To set up the duplicate in Advanced Mode, click Switch to Advanced Mode. See "Duplicating in Advanced Mode" on page 85 for more information.
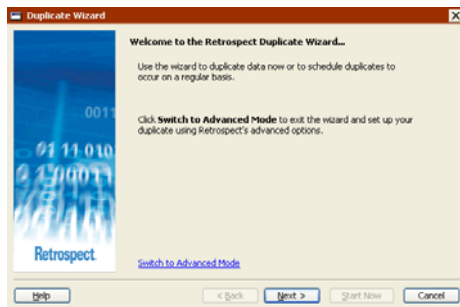
If you have previously set up a duplicate, the welcome screen displays your current settings. See "Editing the Duplicate Settings" on page 84 for more information.

Choosing What to Duplicate

You can now select a specific drive or folder to duplicate.

Click a drive or folder to select it. This deselects any other selected drive or folder.

You can select a drive or folder from any of the containers listed in this screen: My Computer, My Network Places, or Backup Clients.

- To add Retrospect Clients to the Backup Clients container, click Add Clients.
- To add network volumes to the My Network Places container, click Add Network Volumes.
- To display the folders on a drive, select the drive and click Show Folders.

See "Containers" on page 281 for more information.

Choosing File Types to Duplicate

Select the check box for each type of file you want to duplicate. If you select all the check boxes, all files (except cache files) will be duplicated.

NOTE: Some of these options function differently with Windows, Mac OS, NetWare, and UNIX computers. The descriptions below focus on how these options interact with Windows computers. To learn how these options work with other operating systems, see "Built-in Selectors" on page 292.

- **Documents and Settings** duplicates files in the Documents and Settings folder, which contains every user's My Documents, Favorites, Application Data, and Desktop folders.

  NOTE: For Windows 9x systems, the "Documents and Settings" duplicates the "Profiles" folder.

- **Operating System and Applications** duplicates system files, including the Windows folder and the System State. Also duplicates application files, including everything in the Program Files folder, as well as files with known application extensions (like .exe and .dll) anywhere on the source.

  NOTE: If you choose not to duplicate "Operating System and Applications", Retrospect modifies some of its default execution options. Retrospect turns off both the "Duplicate System State" and "Duplicate folder security information for workstations" options. See "Windows System Options" on page 244 and "Windows Security Options" on page 245 for more information.

- **Pictures** duplicates all files in the My Documents\My Pictures folder for all users. It also duplicates files with common picture file extensions (.jpg, for example) anywhere on the source, except the Windows and Program Files folders.

- **Music** duplicates all files in the My Documents\My Music folder for all users. It also duplicates files with common music file extensions (.wma and .mp3, for example) anywhere on the source, except the Windows and Program Files folders.

- **Movies** duplicates all files in the My Documents\My Videos folder for all users. It also duplicates files with common movie file extensions (.mov, for example) anywhere on the source, except the Windows and Program Files folders.

- **Office Documents** duplicates Microsoft Office Documents, Microsoft Outlook data, and Adobe PDF files anywhere on the source, except the Windows and Program Files folders.

- **All Other Files**, duplicates all files not selected by the other options.

NOTE: The Documents and Settings and Operating System and Applications options are not available if you are duplicating a folder.

Choosing the Destination

Select a drive or folder to which you want files duplicated.

NOTE: The destination cannot be the same drive or folder from which files are being duplicated. You *can* duplicate to different folders on the same drive or folders with the same names on different drives.

The Add Clients, Add Network Volumes, and Show Folders buttons on this screen function the same way as in the "What do you want to duplicate?" screen. See "Choosing What to Duplicate" on page 82.

When you click Next, Retrospect displays a dialog warning that the destination folder or drive will be completely replaced with the files you selected to duplicate.

WARNING: Make sure that the destination does not contain any important files before duplicating. Any files already on the destination will be lost and replaced with the files you selected to duplicate. To be safe, create a new folder on the destination drive and duplicate to it.

Click Replace to dismiss the warning and continue setting up the duplicate.

Choosing When to Duplicate

For immediate duplicates, select Now.

If you want to set up a duplicate to run on a schedule, select Later.

The steps to set up a duplicate to run later are described in "Creating a Duplicate Script in Wizard Mode" , starting with "Choosing When to Duplicate" on page 115.

Reviewing the Duplicate Settings

The Duplicate Summary screen displays the duplicate settings you specified in the wizard.
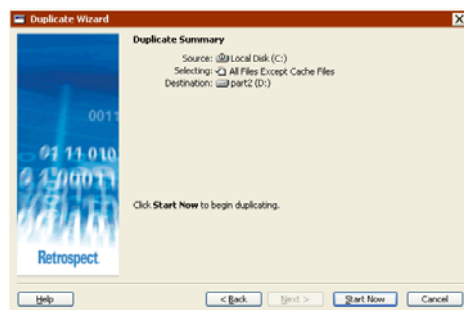
- **Source** lists the drive or folder to duplicate
- **Selecting** lists the file types to duplicate
- **Destination** lists the name of the drive or folder to which data will be copied

To change any of the duplicate settings, click Back.

To start the duplicate, click Start Now

Monitoring the Duplicate

Once you click Start Now, Retrospect exits the Duplicate Wizard and displays the Activity Monitor, just as it would for an immediate duplicate executed from Advanced Mode. See "Monitoring the Duplicate" on page 87 for more information.

Editing the Duplicate Settings

Retrospect automatically remembers the most recent settings you specified for an immediate duplicate. To view and edit those settings choose Backup>Duplicate from the navigation bar.
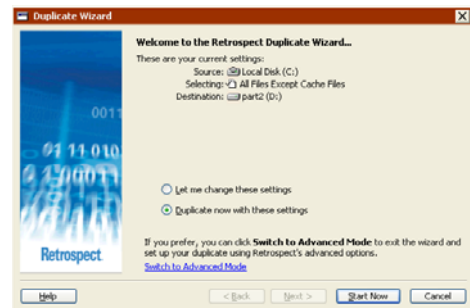
TIP: If the Advanced Mode Duplicate Summary screen displays, click Switch to Wizard Mode.

To duplicate again with the same settings, click Start Now.

To edit the settings, select "Let me change these settings" and click Next. Editing the settings in Wizard Mode is much the same as creating them the first time. See "Duplicating in Wizard Mode" on page 82 for more information.

To edit the settings in Advanced Mode, click "Switch to Advanced Mode". See "Switching from Wizard to Advanced Mode" for more information.

Switching from Wizard to Advanced Mode

To access advanced options that are not available in Wizard Mode, click "Switch to Advanced Mode" from the Welcome screen.

If you have not previously set up a duplicate, you can proceed as described in "Duplicating in Advanced Mode" on page 85.

If you have previously set up a duplicate, Retrospect remembers your settings and displays them in the Advanced Mode summary window.

NOTE: *All* of the Wizard Mode options are available in Advanced Mode. If you switch from Wizard to Advanced Mode, those options are mapped directly to equivalent options.

Duplicating in Advanced Mode

Duplicating in Advanced Mode provides access some powerful Retrospect options that are not available in Wizard Mode. In Advanced Mode you can:

- Access more built-in selectors
- Create and apply custom selectors
- Preview and select specific files to duplicate
- Choose a duplicate method
- Set many additional options not available in Wizard Mode

To set up an Immediate Duplicate in Advanced Mode, click Backup from the navigation bar, then click the Duplicate button.

If the Duplicate Wizard welcome screen displays, click Switch to Advanced Mode. The Immediate Duplicate summary window displays.
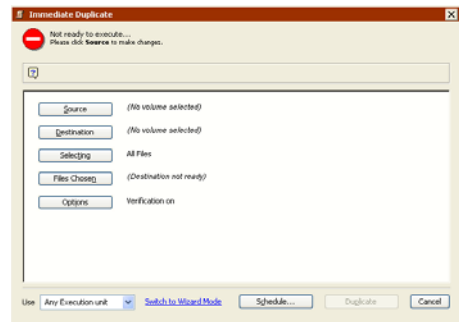
Click the buttons on the summary screen to specify the source, destination, and other backup options.

Choosing the Source Volume

In the Immediate Duplicate summary window, click the Source button to display the Source Selection window.
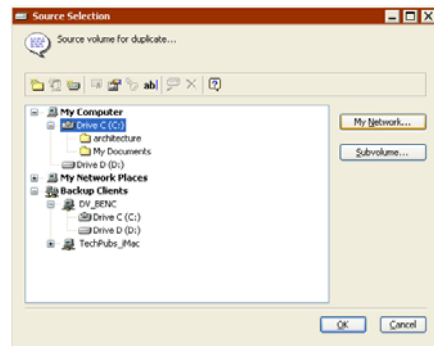
Select the source volume from which files will be copied and click OK. For details on using the source selection window, see "Working with Volumes" on page 280.

Choosing the Destination

In the Immediate Duplicate summary window, click the Destination button to display the Source Selection window again.
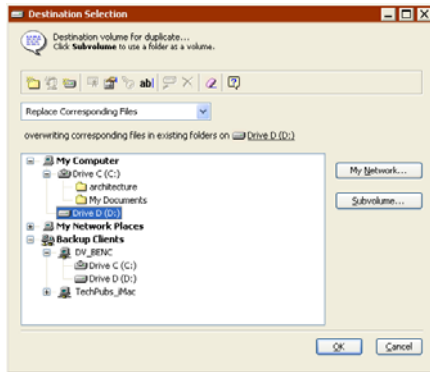
Select a destination volume and choose a duplicate method from the list box.

Replace Entire Volume *replaces the entire contents* of the destination volume with the selected files and folders from the source volume. Identical files already present on the destination are not duplicated.

Replace Corresponding Files copies the selected files and folders to the destination volume. When Retrospect finds a file that exists on both the source and destination, the destination file is *always* overwritten. Retrospect leaves files untouched if they are identical to files marked for duplication or if the file names and locations do not match those marked.

Replace if Source is Newer copies the selected files and folders to the destination volume. When Retrospect finds a file that exists on both the source and destination, the destination file is overwritten *only if the source file is newer*. Retrospect leaves files untouched if they are identical to files marked for duplication or if the file names and locations do not match those marked.

Duplicate Missing Files Only, copies only the selected files and folders that don't already exist on the destination volume. Other files and folders on the destination are left untouched.

When you have selected the volume and set the list box click OK.

Setting Additional Options

After you have specified the source volume to duplicate and the destination volume to which files will be copied, use the Immediate Duplicate summary window to verify your choices and set additional options.
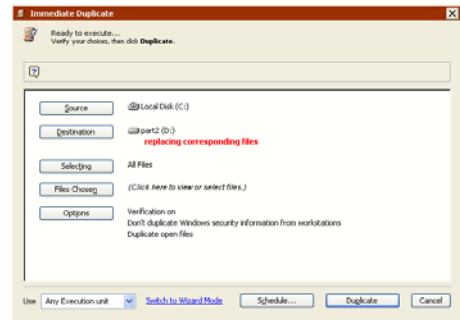
To makes changes, click the appropriate button.

Source lets you change the source volume or folder.

Destination lets you choose a different volume or folder as the destination.

Selecting lets you choose a selector, a kind of filter for selecting files and folders to be duplicated. (Selectors are explained in detail in "Using Selectors" on page 291.) The default selector is "All Files Except Cache Files" which duplicates all files on the source.

Files Chosen scans the source volume and determines which files need to be duplicated by comparing the source files against the files that already exist on the destination. When the scan is complete, Retrospect opens a browser window to display a list of the files on the source volume marked for duplicate. You can use it to mark and unmark individual files and folders to be duplicated.

Browsers are explained in "Browsing" on page 286. When you close the browser, the summary window displays information about the selected files.

Options displays the basic options window in which you can turn verification on or off and choose whether or not to update the backup report. See "Duplicate Execution Options" on page 239 for more information.
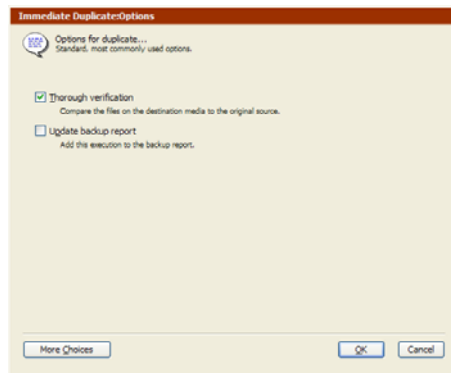
Click the More Choices button to access many more options. See "Execution Options" on page 236 for more information.

Executing the Duplicate

If Retrospect has the information it needs, it says "Ready to Execute" at the top of the Immediate Duplicate summary window. If the information is incomplete, it says "Not Ready to Execute" and you must change one or more parts of the information you gave it.

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this operation (or choose "Any Execution unit"). Make your selection in the summary window's combo box. See "Assigning Execution Units" on page 162 for more information.

When you are ready, click Duplicate.

WARNING: Duplicating may destroy data on the destination. Be sure it is acceptable to erase or replace files on the destination volume.

Monitoring the Duplicate

The Activity Monitor window shows the progress of the duplicate operation and includes buttons to pause or stop its execution.
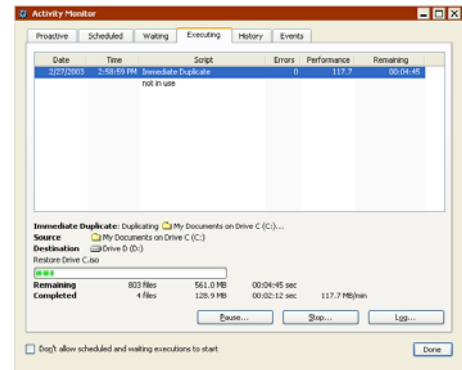
When the execution is complete, click the History tab to see performance data for the duplicate operation. If any errors occurred you get more information by clicking the Errors button. To view the Operations Log for this execution, click the Log button.

This log is described in "Viewing the Operations Log" on page 231.

Editing the Duplicate Settings

Retrospect automatically remembers the most recent settings you specified for an immediate duplicate. To view and edit those settings choose Backup>Duplicate from the navigation bar.
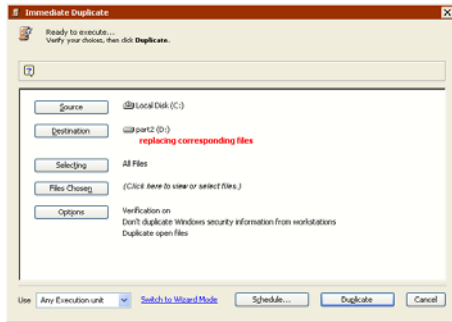
TIP: If the Wizard Mode duplicate summary screen displays, click Switch to Wizard Mode.

To duplicate again with the same settings, click Duplicate.

To edit the settings, click the buttons to change the source, destination, file selection criteria, and options. Editing the settings in Advanced Mode is the same as creating them the first time. See "Duplicating in Advanced Mode" on page 85 for more information.

To edit the settings in Wizard Mode, click "Switch to Wizard Mode". See "Switching from Advanced to Wizard Mode" for more information.

Scripting the Duplicate

If you want to automate your duplicates so they can be performed while your computer is unattended (e.g., when you go home at night), you can use Retrospect's scripting feature to set up and schedule duplicates.

From the Immediate Duplicate summary window, click the Schedule button to save the immediate duplicate information and settings as a script. You can then add a schedule to the script to accomplish automatic, unattended duplicate operations.

See "Scheduling Scripts" on page 134.

Switching from Advanced to Wizard Mode

In general, Tqzkq recommends editing immediate duplicates in the same mode you created them. Of course, you can switch between the modes and if you do, it's important to know how Retrospect handles advanced options that are not available in Wizard Mode.

To return to Wizard Mode at any time, click "Switch to Wizard Mode" from the Advanced Mode summary window.

If you have made any changes to your duplicate settings, Retrospect asks if you want to save those changes before switching modes.
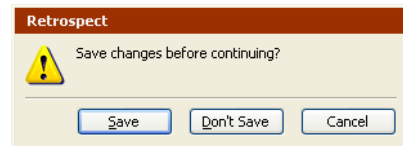
If you have not made any changes, Retrospect displays the Wizard Mode Welcome screen with a summary of the current duplicate settings.

Since Advanced Mode includes options not available in Wizard Mode, Retrospect must either keep those settings, or discard them. There are a few important options to consider:

• Duplicate Method
• Selectors
• Execution Options
• Manual File Selection
• Execution Unit

Duplicate Method

When choosing the destination in Advanced Mode, Retrospect lets you specify the method by which files are copied. You can choose:

• Replace Entire Volume
• Replace Corresponding Files

- Replace if Source is Newer
- Duplicate Missing Files Only

You cannot specify a duplicate method in Wizard Mode; it always uses the Replace Entire Volume method.
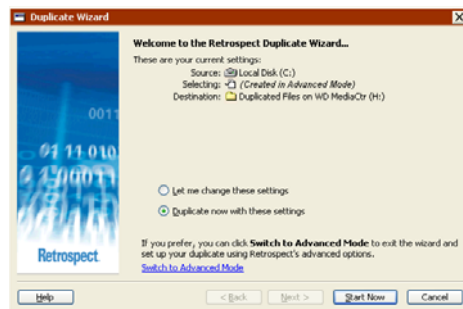
For more information on the difference between the duplicate methods, see "Choosing the Destination" on page 85.
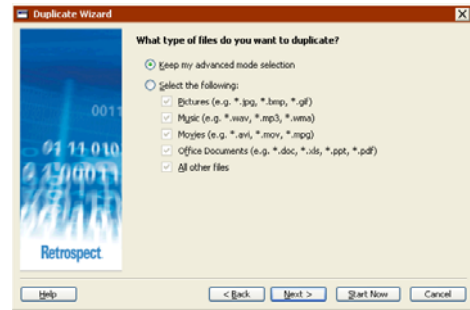
Selectors

Advanced Mode includes a number of built-in selectors that are not available in Wizard Mode. In addition, you can create and use custom selectors in Advanced Mode.

If you choose a selector that is not available in Wizard Mode, then click "Switch to Wizard Mode", Retrospect *keeps* the advanced selector and applies it when you run the duplicate.

In these situations, the Wizard Mode Welcome screen displays *(Created in Advanced Mode)* in the Selecting field.

In addition, if you edit your duplicate settings, a new option appears in the "What type of files do you want to duplicate?" screen.

- Choose "Keep my advanced mode selection" to keep your advanced selector.
- Choose "Select the following" and select a new option to discard the advanced selector and use a new one.

Execution Options

Advanced Mode includes many execution options that are not available in Wizard Mode, such as verification.

If you choose an execution option that is not available in Wizard Mode, then click "Switch to Wizard Mode", Retrospect *keeps* the advanced execution option and applies it when you run the duplicate.

WARNING: The Wizard Mode Welcome screen does not indicate whether the duplicate includes advanced execution options or not. The only way to check is to switch to Advanced Mode and review the Options settings.

Manual File Selection

In Advanced mode, you can click the Files Chosen button and select specific files and folders to duplicate. If you do this, the Advanced Mode summary window displays *(Manual selection)* in the Selecting field.
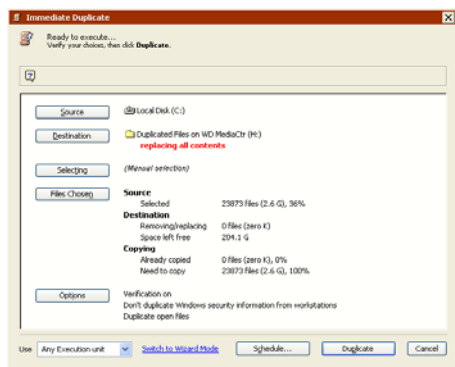
If you apply a manual selection, then click "Switch to Wizard Mode", Retrospect *discards* the selection. There is no way to perform manual selection in Wizard Mode.

Execution Unit

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for a duplicate operation in Advanced Mode only.

If you choose a specific execution unit (not "Any Execution unit"), then click "Switch to Wizard Mode", Retrospect *keeps* the execution unit information and uses the specific execution unit when you run the duplicate.

NOTE: The Wizard Mode Welcome screen does not indicate whether the duplicate specifies an execution unit or not. The only way to check is to switch to Advanced Mode and review the settings.

TRANSFER BACKUP SETS

Retrospect's Transfer Backup Sets function copies all files and Snapshots from one or more Backup Sets to a single new or existing Backup Set. It can be used to:

- Clone a Backup Set
- Protect against media failure
- Provide for offsite storage

- Start a new cycle of backups
- Consolidate multiple Backup Sets to a single Backup Set

As with backup operations, transferring Backup Sets by default matches files in the source to files already in the destination and only copies the necessary files. Existing Snapshots and files on the destination remain untouched.

The Transfer Backup Sets function does not have a preview feature. You must rely on selectors instead of picking and choosing files by hand.

To transfer files between Backup Sets, you must have a separate tape or CD/DVD drive for each Backup Set, even if both Backup Sets are on the same type of media. In the case of disk and file Backup Sets the need for separate backup devices does not apply.

TIP: If you do not have separate drives for each Backup Set, you can first transfer files temporarily to a disk Backup Set and then transfer the disk Backup Set to the final destination Backup Set.

To transfer files between Backup Sets, click Tools>Transfer Backup Sets. The Backup Set Transfer summary window displays.
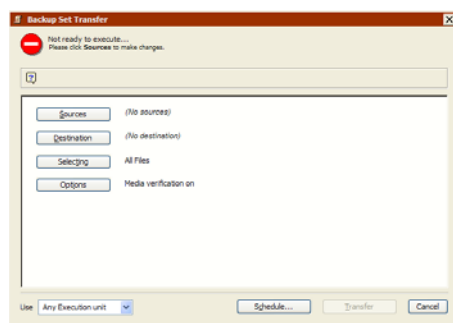

The basic steps in transferring Backup Sets are:

- Selecting the Source Backup Sets
- Selecting the Destination Backup Set

- Selecting Files to Transfer
- Setting Additional Options
- Executing the Backup Set Transfer
- Scripting the Backup Set Transfer

Selecting the Source Backup Sets

In the Backup Set Transfer summary window, click Sources to display the Backup Set Selection window.
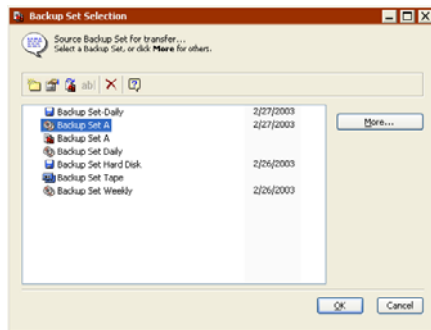
Select one or more source Backup Sets, and click OK.

NOTE: Backup Set Transfer copies *all* Snapshots and associated files in the source Backup Set(s) to the destination Backup Set. This is different from Snapshot Transfer, which copies only *active* Snapshots and associated files. See "Transfer Snapshots" on page 92 for more information.

Selecting the Destination Backup Set

In the Backup Set Transfer summary window, click Destination.

Select the destination Backup Set and click OK. If the only Backup Sets listed in the window are already specified as the source, or if you do not want to use any of the Backup Sets in the list as the destination, click Create New to create a new Backup Set. See "Creating Backup Sets" on page 252 for more information.

Selecting Files to Transfer

By default, Retrospect transfers all files from the source Backup Sets to the destination Backup Set. To transfer a subset of all files, click Selecting in the Backup Set Transfer summary window.

Choose a selector from the list or click More Choices to create a custom selector. Selectors are a kind of filter for selecting files and folders to be transferred. Selectors are explained in detail in "Using Selectors" on page 291.

Click OK when done.

Setting Additional Options

Retrospect includes a number of execution options that are specific to Backup Set Transfers.

Click Options in the Backup Set Transfer summary window to change the default settings for the Copy Snapshots, Media verification, Data compression, Recycle source Backup Set, and other options.

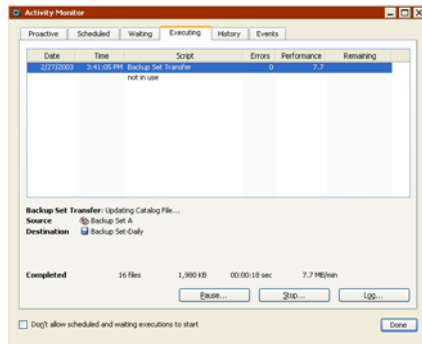See "Transfer Execution Options" on page 239 for more information about these options.

Click the More Choices button to access additional execution options. See "Execution Options" on page 236 for more information.

Executing the Backup Set Transfer

If Retrospect has the information it needs, it says "Ready to Execute" at the top of the Backup Set Transfer summary window. If the information is incomplete, it says "Not Ready to Execute" and you must change one or more parts of the information you gave it.

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this operation (or choose "Any Execution unit"). Make your selection in the summary window's combo box. See "Assigning Execution Units" on page 162 for more information.

When you are ready, click Transfer. Retrospect performs the transfer operation, displaying its progress in the Activity Monitor window.

Retrospect may ask you to insert media.

When the execution is complete, click the History tab to see performance data for the transfer operation. If any errors occurred you get more information by clicking the Errors button. To view the Operations Log for this execution, click the Log button.

This log is described in "Viewing the Operations Log" on page 231.

Scripting the Backup Set Transfer

When a Backup Set Transfer summary window is active, you can click the Schedule button to save the transfer information and settings as a script. You can then use the script to accomplish Backup Set Transfer operations.

See Chapter 5 • Automated Operations.

TRANSFER SNAPSHOTS

Retrospect's Transfer Snapshots function copies Snapshots and their associated files from one Backup Set to a new or existing Backup Set. It can be used to:

- Start a new Backup Set with a synthetic full backup
- Create an offsite disaster recovery Backup Set
- Start a new cycle of backups with a full backup

Transfer Snapshots is different from Transfer Backup Sets in a number of ways. Transfer Snapshots:

- Can only have a single Backup Set as the source; Transfer Backup Sets can have multiple sources.
- Transfer only *active* Snapshots; Transfer Backup Sets transfers *all* Snapshots.
- Provides different methods for selecting which Snapshots get transferred; Transfer Backup Sets always transfers *all* Snapshots.

By default, transferring Snapshots matches files in the source to files already in the destination and only copies the necessary files. Existing Snapshots and files on the destination remain untouched.

The Transfer Snapshots function does not have a preview feature. You must rely on selectors instead of picking and choosing files by hand.

To transfer Snapshots between Backup Sets, you must have a separate tape or CD/DVD drive for each Backup Set, even if both Backup Sets are on the same type of media. In the case of disk and file Backup Sets the need for separate backup devices does not apply.

TIP: If you do not have separate drives for each Backup Set, you can first transfer Snapshots temporarily to a disk Backup Set and then transfer the disk Backup Set Snapshots to the final destination Backup Set.

Snapshot Transfer and Synthetic Fulls

The Snapshot transfer feature allows you to create what Retrospect calls a "synthetic full" backup. Retrospect creates synthetic fulls when transferring Snapshots to:

• A new Backup Set
• An existing Backup Set when the "Match source Catalog File to destination Catalog File" option is turned off

Synthetic fulls allow you to quickly seed a new Backup Set with only the most recent Snapshots (for example) from an existing Backup Set. This allows you to start a fresh cycle of backups without losing the time-saving benefits of Progressive Backup. Subsequent backups to the new Backup Set will copy only new and changed files.

After the transfer, the destination Backup Set contains the same data it would after a full backup. You get a full backup without having to perform the more time-consuming process of executing a *actual* full backup.

NOTE: A synthetic full backup is the equivalent of a full backup done *at the time of* the most recent Snapshots. It does not include files that are new or changed since the date and time of those Snapshots, nor does it include older versions of files contained in non-current Snapshots.

Synthetic fulls are also useful for creating a Backup Set that contains all its files in one contiguous session. This allows Retrospect to restore entire volumes more quickly, since it does not have to search through multiple sessions to find all the required files.

To transfer Snapshots between Backup Sets, click Tools>Transfer Snapshots. The Backup Set Snapshot Transfer summary window displays.
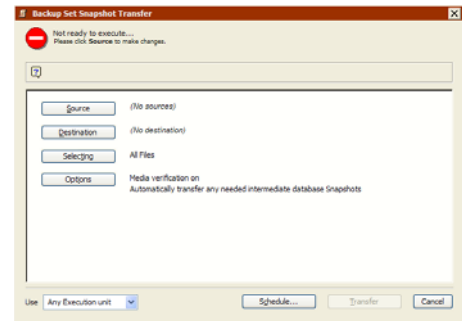

The basic steps in transferring Snapshots are:

• Selecting the Source Backup Set
• Selecting Snapshots
• Selecting the Destination Backup Set
• Selecting the Files to Transfer
• Setting Additional Options
• Executing the Snapshot Transfer
• Scripting the Snapshot Transfer

Selecting the Source Backup Set

In the Backup Set Snapshot Transfer summary window, click Sources to display the Transfer Snapshots source selection.
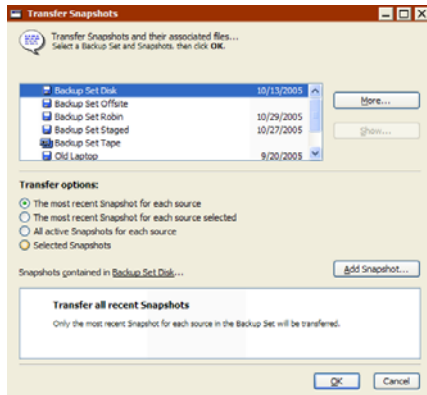
In the source selection window's top list, select the Backup Set containing the Snapshot(s) you want to transfer. Click the More button if your desired Backup Set is not listed.

TIP: If you want to transfer Snapshots from more than one Backup Set at one time, use Transfer Backup Sets instead, or create a Transfer Snapshots script. See "Transfer Backup Sets" on page 90 and "Scripted Snapshot Transfer" on page 127.

Retrospect displays a list of the selected Backup Set's *active* Snapshots in the window's bottom list, along with the date and time of the Snapshot and the name of the backed up volume.

NOTE: The list of Snapshots is only displayed if you select one of the following options: "Selected Snapshots" or "The most recent Snapshot for each source selected". Only Backup Sets with a date next to them contain Snapshots.

By default, Retrospect saves the most recent Snapshot for each volume (or subvolume) that was backed up in its Catalog File. These Snapshots are considered *active*. All Snapshots, including older ones, are saved on the backup media (tape, disk, or CD/DVD). Following each successful backup or archive operation, the old Snapshot is replaced in the Catalog File with the new one. The old Snapshot remains untouched

on the backup media and can be retrieved when needed.

NOTE: A disk Backup Set with grooming enabled saves all the Snapshots required by its grooming policy in the Catalog File. For example, if you told Retrospect to save the last 10 backups, then up to ten Snapshots for each volume will be active. In addition, any Snapshots that have been manually locked are also active.

If the Snapshot you want to transfer is not listed, click the Add Snapshot button to display a list of all Snapshots in the Backup Set.

When you select a Snapshot and click Retrieve Retrospect obtains the older Snapshot from the Backup Set media (which may require you to insert media) and adds it to the list in the Transfer Snapshots source window. That Snapshot is now *active*.

NOTE: The Retrieve button is disabled when you select a Snapshot that is already available.

Selecting Snapshots

Once you select a source Backup Set, there are a number of ways to select which Snapshots to transfer.

• **The most recent Snapshot for each source** transfers the most recent Snapshot for each volume (or subvolume) in the active Snapshots list.

• **The most recent Snapshot for each source selected** transfers the most recent Snapshot for each volume (or subvolume) you select in the active Snapshots list. You could manually select the most current Snapshot for each volume to achieve the same effect.

• **All active Snapshots for each source** transfers all *active* Snapshots and associated files. To see the list of active Snapshots and their sources, temporarily choose the "Selected Snapshots" option. Make sure to

choose "All active Snapshots for each source" again before clicking OK. To make an older Snapshot active, click Add Snapshot.

- **Selected Snapshots** transfers only those Snapshots (and associated files) that you select from the active Snapshots list. Control-click or Shift-click to select multiple Snapshots. To make an older Snapshot active, click Add Snapshot.

"The most recent Snapshot..." options are most useful for Transfer Snapshots scripts (since the list of active Snapshots changes each time you back up), but also have some application for immediate operations.

NOTE: Transfer Snapshots only copies *active* Snapshots. To copy *all* Snapshots, use Transfer Backup Sets. See "Transfer Backup Sets" on page 90 for more information.

When you have made your selections, click OK.

Selecting the Destination Backup Set

In the Backup Set Snapshot Transfer summary window, click Destination.

Select the destination Backup Set and click OK. If you do not want to use any of the Backup Sets in the list as the destination, click Create New to create a new Backup Set. See "Creating Backup Sets" on page 252 for more information.

Selecting the Files to Transfer

By default, Retrospect transfers all files from the selected Snapshots to the destination Backup Set. To transfer a subset of all files, click Selecting in the Backup Set Snapshot Transfer summary window.

Choose a selector from the list or click More Choices to create a custom selector. Selectors are a kind of filter for selecting files and folders to be transferred. Selectors are explained in detail in "Using Selectors" on page 291.

Click OK when done.

Setting Additional Options

Retrospect includes a number of execution options that are specific to Snapshot transfers.

Click Options in the Backup Set Snapshot Transfer summary window to change the default settings for the Media Verification, Data compression, Recycle source Backup Set, and other options.
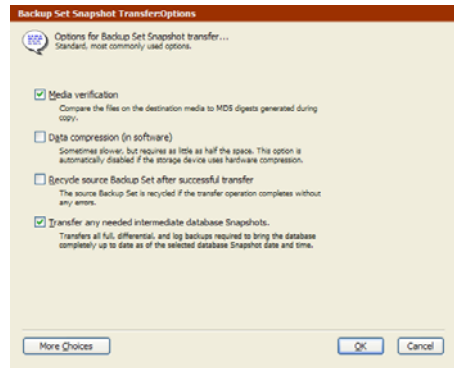
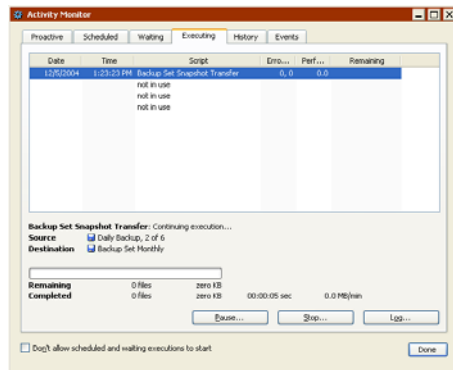See "Transfer Execution Options" on page 239 for more information about these options.

Click the More Choices button to access additional execution options. See "Execution Options" on page 236 for more information.

Executing the Snapshot Transfer

If Retrospect has the information it needs, it says "Ready to Execute" at the top of the Backup Set Snapshot Transfer summary window. If the information is incomplete, it says "Not Ready to Execute" and you must change one or more parts of the information you gave it.

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this operation (or choose "Any Execution unit"). Make your selection in the summary window's combo box. See "Assigning Execution Units" on page 162 for more information.

When you are ready, click Transfer. Retrospect performs the transfer operation, displaying its progress in the Activity Monitor window.

Retrospect may ask you to insert media.

When the execution is complete, click the History tab to see performance data for the transfer operation. If any errors occurred you get more information by clicking the Errors button. To view the Operations Log for this execution, click the Log button.

This log is described in "Viewing the Operations Log" on page 231.

Scripting the Snapshot Transfer

When a Backup Set Snapshot Transfer summary window is active, you can click the Schedule button to save the transfer information and settings as a script. You can then use the script to accomplish Snapshot Transfer operations.

See Chapter 5 • Automated Operations.

CONTROLLING IMMEDIATE OPERATIONS

Retrospect gives you a number of ways to control an immediate operation while it's in progress. See Chapter 6 • Controlling Operations for more information.

You can use the "Stay in Retrospect" combo box in Retrospect's toolbar to determine what Retrospect does when it is finished executing an immediate operation. By default, Retrospect does nothing, but if you want to start an immediate operation and then go home, you can choose to have Retrospect quit when the execution is complete. Unless Proactive Backup is running, or another script is scheduled to run in the application's look ahead time, Retrospect will quit (or shut down) when done. See "Schedule Preferences" on page 264 for more information on specifying the look ahead time.

AUTOMATED OPERATIONS

- **OVERVIEW OF SCRIPTS**

- **CREATING SCRIPTS**

- **SCRIPTED BACKUP**

- **SCRIPTED DUPLICATE**

- **SCRIPTED ARCHIVE**

- **SCRIPTED RESTORE**

- **SCRIPTED BACKUP SET TRANSFER**

- **SCRIPTED SNAPSHOT TRANSFER**

- **SCRIPTED GROOMING**

- **SCRIPTED VERIFICATION**

- **SCHEDULING SCRIPTS**

- **SAVING SCRIPTS**

- **TESTING SCRIPTS**

- **EXECUTING SCRIPTS**

- **CONTROLLING SCRIPTS**

- **PROACTIVE BACKUP SCRIPTS**

You learned how to set up and execute Retrospect's immediate backup, duplicate, archive, restore, and transfer operations in Chapter 4 • Immediate Operations. This chapter shows you how to automate the process by using scripts, including Retrospect's unique Proactive Backup scripts.

OVERVIEW OF SCRIPTS

One of the advantages of Retrospect is its ability to automate repetitive tasks. By creating scripts, you can automate all of the operations described in Chapter 4 • Immediate Operations, namely:

- Backing up
- Duplicating
- Archiving
- Restoring
- Transferring Backup Sets
- Transferring Snapshots

In addition, Proactive Backup allows you to create intelligent scripts that continually reprioritize which computers get backed up next based on criteria you specify. You can also create Groom scripts and Verification scripts to automate these Backup Set management tasks.

Scripts are an important part of developing a backup strategy. For more information on developing an effective backup strategy, see "Backup Strategies" on page 224.

Automated operations include all of the same information as immediate operations: a source, destination, file selection criteria, and other options. Scripts also include a scheduling component that controls when these automated operations are executed.

Retrospect allows you to schedule scripts to run automatically and unattended so you can choose operating times that are most convenient for you and for other users. Scheduling scripted backups ensures data is backed up consistently—all you have to do is make sure the backup computer is turned on and the proper media is in the backup device. When it is time for a script to execute, Retrospect automatically launches and executes the operation. If there are no other scripts scheduled to run in Retrospect's look ahead time, and you selected "shut down when done" in the Startup Preferences, Retrospect shuts down when the operation is complete.

Automated Operations covers creating scripts, scheduling scripts, executing scripts, and working with Proactive Backup Scripts. For information on managing and maintaining scripts, see "Maintaining Scripts" on page 261.

CREATING SCRIPTS

There are two ways to create scripts in Retrospect:

- Scheduling an Immediate Operation
- Using the Manage Scripts Command

Using these methods you can create any type of script, including backup, duplicate, archive, restore, and transfer.

NOTE: Proactive Backup Scripts are discussed separately. See "Proactive Backup Scripts" on page 140 for more information.

Scheduling an Immediate Operation

All the immediate operation summary windows (Backup, Duplicate, Archive, Restore, and Transfer) include a Schedule button that allows you to create a script based on that operation.

NOTE: For backup, duplicate, and restore operations, you must be in Advanced Mode to access the Schedule button.

To Schedule an Immediate Operation:

1. Click the Schedule button from an immediate operation summary window.

2. Enter a name for the script and click OK.

3. Verify or modify the information in the script summary window.

4. Click the Schedule button and schedule the script as described in "Scheduling Scripts" on page 134.

5. When all the information in the script summary window is correct, click the Save icon 🖫 in the toolbar.

You can also create backup scripts from the immediate Backup Wizard and duplicate scripts from the immediate Duplicate Wizard. See "Backing Up in Wizard Mode" on page 54 and "Duplicating in Wizard Mode" on page 82 for more information.

Using the Manage Scripts Command

You can use the Manage Scripts command to create a new script or to modify the settings of an existing script.

For more information on how to modify existing scripts, see "Maintaining Scripts" on page 261. For information on creating new scripts, see the following sections:

- Scripted Backup
- Scripted Duplicate
- Scripted Archive
- Scripted Restore
- Scripted Backup Set Transfer
- Scripted Snapshot Transfer
- Scripted Grooming
- Scripted Verification

For information about Restore Database and Restore Mailbox scripts, see Appendix A: SQL Server Agent and Appendix B: Exchange Server Agent.

SCRIPTED BACKUP

There are two ways to set up a scripted backup using the Manage Scripts command. You can use Retrospect's Backup Wizard, which walks you through the process of setting up a scripted backup, or you can set up the backup on your own in Advanced Mode. Advanced Mode has options that are unavailable in the Wizard. For more information see:

- Creating a Backup Script in Wizard Mode
- Switching from Wizard to Advanced Mode
- Creating a Backup Script in Advanced Mode
- Switching from Advanced to Wizard Mode

Creating a Backup Script in Wizard Mode

The Backup Wizard provides an easy way to set up and edit scripted backup operations. To start the Backup Wizard, click Automate from the navigation bar, then click the Manage Scripts button. The script editing window displays.
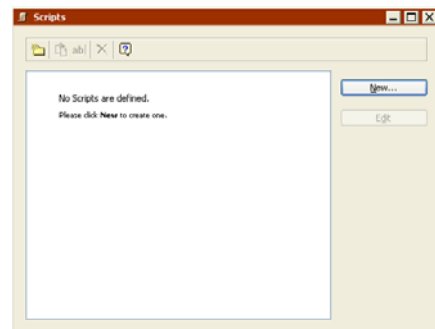
Click the New button to create a new script. The script selection window displays.
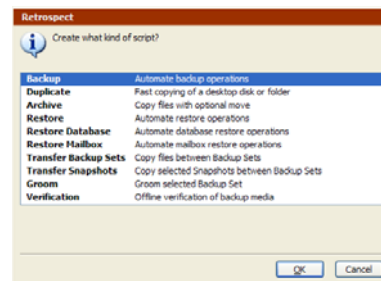
Select Backup from the list and click OK. In the script naming window, enter a name and click OK. The Backup Wizard welcome screen displays.

NOTE: If the Advanced Mode Backup Script summary screen displays, click Switch to Wizard Mode.
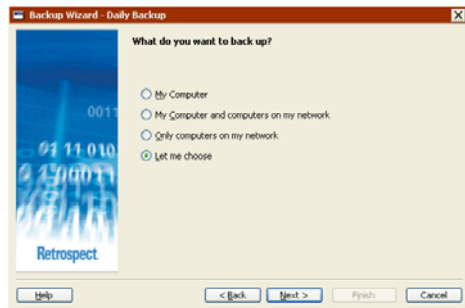
Welcome Screen

If this is the first time you are setting up a scripted backup, click Next to continue set up using the Backup Wizard. To set up the backup in Advanced Mode, click Switch to Advanced Mode. See "Creating a Backup Script in Advanced Mode" on page 107 for more information.
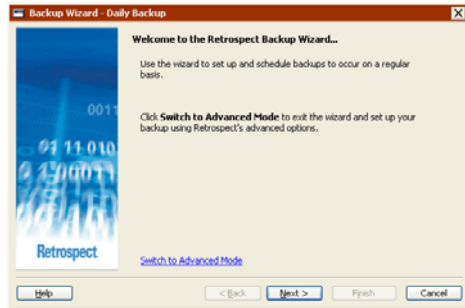
If you have previously set up a scripted backup, the welcome screen displays your current settings. See "Editing the Backup Script Settings" on page 106 for more information.

Choosing What to Back Up

Click the option button that describes what you want to back up.

- **Documents and Settings,** (only available for Retrospect Professional) backs up the Documents and Settings folder, which contains every users' folders, including My Documents, Pictures, Music, Favorites, and Desktop.

- **My Computer**, backs up the local computer.
- **My Computer and computers on my network**, backs up the local computer and all logged in Retrospect Client computers.
- **Only computers on my network**, (not available for Retrospect Professional) backs up all logged in Retrospect Client computers.
- **Let me choose**, allows you to select the drives and folders you want to back up from the local computer, logged in Retrospect Client computers, and network volumes.

Adding Retrospect Clients

If you chose to back up "My Computer and computers on my network" or "Only computers on my network", Retrospect will back up data from all Retrospect Client computers logged in at the time of the backup.

To log in Retrospect Clients now, click Add Clients. For more information on installing, configuring, and logging in clients, see Chapter 7 • Networked Clients.

Choosing Specific Drives or Folders

If you selected "Let me choose" in the "What do you want to back up?" screen, you can now select one or more specific drives or folders to back up.

Click a drive or folder to select it. This deselects any other selected drive or folder. Press and hold the Control key and click a drive or folder

to select it without deselecting any current selections. Press and hold the Shift key and click a drive or folder to select all drives and folders listed from the current selection to the Shift-clicked selection.

You can select drives and folders from any of the containers listed in this screen: My Computer, My Network Places, Backup Clients, and Source Groups. You can also select one or more of the containers themselves to back up everything inside.

- To add Retrospect Clients to the Backup Clients container, click Add Clients.
- To add network volumes to the My Network Places container, click Add Network Volumes.
- To display the folders on a drive, select the drive and click Show Folders.

See "Containers" on page 281 for more information.

Choosing File Types to Back Up
Select the check box for each type of file you want to back up. If you select all the check boxes, all files (except cache files) will be backed up.

NOTE: Some of these options function differently with Windows, Mac OS, NetWare, and UNIX computers. The descriptions below focus on how these options interact with Windows computers. To learn how these options work with other operating systems, see "Built-in Selectors" on page 292.

- **Documents and Settings** backs up files in the Documents and Settings folder, which contains every user's My Documents, Favorites, Application Data, and Desktop folders.

  NOTE: For Windows 9x systems, the "Documents and Settings" backs up the "Profiles" folder.

- **Operating System and Applications** backs up system files, including the Windows folder and the System State. Also backs up application files, including everything in the Program Files folder, as well as files with known application extensions (like .exe and .dll) anywhere on the source.

  NOTE: If you choose not to back up "Operating System and Applications", Retrospect modifies some of its default execution options. Retrospect turns off both the "Back Up System State" and "Back up folder security information for workstations" options. See "Windows System Options" on page 244 and "Windows Security Options" on page 245 for more information.

- **Pictures** backs up all files in the My Documents\My Pictures folder for all users. It also backs up files with common picture file extensions (.jpg, for example) anywhere on the source, except the Windows and Program Files folders.

- **Music** backs up all files in the My Documents\My Music folder for all users. It also backs up files with common music file extensions (.wma and .mp3, for example) anywhere on the source, except the Windows and Program Files folders.
- **Movies** backs up all files in the My Documents\My Videos folder for all users. It also backs up files with common movie file extensions (.mov, for example) anywhere on the source, except the Windows and Program Files folders.
- **Office Documents** backs up Microsoft Office Documents, Microsoft Outlook data, and Adobe PDF files anywhere on the source, except the Windows and Program Files folders.
- **All Other Files**, backs up all files not selected by the other options.

NOTE: The Documents and Settings and Operating System and Applications options are not available if you are backing up a folder.

Choosing the Backup Destination Device

You can store your backup on any device supported by Retrospect, including tape drives, CD/DVD drives, and hard drives. Select one of the following options:

- Tape, CD, DVD
- Hard drives on the local computer or on the network

For Tape/CD/DVD, Retrospect displays the available devices. Select the device to which you want to back up and click Next.

For hard drives, Retrospect displays local hard drives and any network volumes listed in the My Network Places container.

To add a network volume, double-click My Network Places, then navigate to the volume you want to add, select it, and click the Add but-

ton. If the volume requires it, enter a login and password and click OK.

NOTE: If you set up Retrospect to log in as a user with privileges to the network volume, you will not be prompted to log in again. See "Security Preferences" on page 265 for more information.

To specify a folder on a local drive or network volume, select it, then click the Browse button. Navigate to the folder you want to back up to and click OK.

Choosing Whether to Create a Schedule

You can either create a script with a schedule or without a schedule.

If you choose not to create a schedule, you can still run the script manually at any time. See "Manual Script Execution" on page 139 for more information. You can also add a schedule to the script later.

Make a selection and click Next.

NOTE: If you are editing a script that already has a schedule, an additional option, "Keep the existing schedule", is also available.

Choosing When to Back Up

Select the check box for each day you want the backup script to run and specify a time for the script to start.
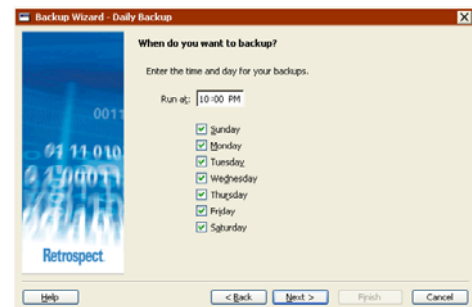
TIP: Although Retrospect can back up computers while they are in use, it is a good idea

to run scripts after normal business hours when computers tend to be less busy.

Specifying One or Multiple Backup Sets

Choose whether you always want to back up to one Backup Set, or want to use multiple Backup Sets.

Backing up to multiple Backup Sets increases the level of protection. Since each set contains a complete backup of your data, you have a built-in safety net in case of media failure. In addition, with multiple Backup Sets, you can move the media for a Backup Set that is not currently in use to an offsite location for protection against theft, fire, or other disasters.

NOTE: If you chose to back up on only one day of the week, this screens lets you choose to back up to one Backup Set or two Backup Sets (alternating between Backup Sets each week).

Choosing the Number of Backup Sets

If you chose to back up to multiple Backup Sets, you can now specify how many Backup Sets you want to use and how often you want to alternate between backing up to each of them.

The first option alternates between Backup Sets on each day you chose to back up. For example, if you chose to back up every day of the week, Retrospect gives you the option to back up to seven Backup Sets. In this case, Retrospect backs up to a different Backup Set each day of the week. If you choose to back up Monday, Wednesday, and Friday, Retrospect gives you

the option to back up to three Backup Sets and uses a different one every Monday, Wednesday, and Friday.

The second option always uses two Backup Sets and alternates between them each week. For example, if you choose to back up every day of the week, Retrospect backs up to one Backup Set every day in the first week, then backs up to the other Backup Set every day in the next week. If you select this option, use the list box to specify the day of the week on which you want to switch between Backup Sets.

Naming the Backup Set(s)

This screen varies based on the number of Backup Sets you specified.

Enter as many Backup Set names as required, or use the default names provided by Retrospect. If you have already created any Backup Sets, you can select the "Use Existing" check box and choose a Backup Set from the list box.

TIP: If you are using multiple Backup Sets, it is especially important to give them meaningful names. You will *not* be able to rename the Backup Sets later.

NOTE: The "Use Existing" check box only appears if you have existing Backup Sets.

Setting the Compression Option

Click the "Yes" option button to turn on software data compression for this backup script.

Data compression saves space in the Backup Set by compressing files before copying them into the Backup Set. Files are automatically de-compressed back to their original state when restored.

The amount of compression savings you can expect depends on the types of files you are compressing. Text files compress substantially, application and system files do not.

Backups (and restores) from Backup Sets using data compression are slower than those that do not.

NOTE: When copying to a tape device that has built-in hardware data compression, Retrospect automatically turns off software compression and always uses hardware compression for best performance.

Setting Backup Set Security Options

This screen allows you to specify a password to restrict access to the Backup Set(s). You can also choose to encrypt the Backup Set data to provide additional security.

NOTE: Using encryption increases backup time.
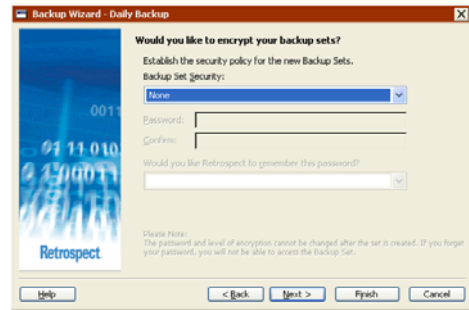
Choose an option from the Backup Set Security list box.

- **None**: provides no password protection for the Backup Set(s) and does not encrypt the Backup Set data.
- **Password only**: provides password protection for the Backup Set(s). Stored data is not encrypted.
- **SimpleCrypt**: provides password protection and encrypts Backup Set data using Retrospect's proprietary encryption format.
- **DES**: provides password protection and encrypts Backup Set data using the Data Encryption Standard.
- **AES-128**: provides password protection and encrypts Backup Set data using the Advanced Encryption Standard (128 bit).
- **AES-256**: provides password protection and encrypts Backup Set data using the Advanced Encryption Standard (256 bit). AES-256 provides the best combination of security and performance.

WARNING: Once a Backup Set is password-protected or encrypted, you *cannot* change these settings. In addition, if you forget your password, you will not be able access the Backup Set.

If you set a password and want Retrospect to re-member it under certain circumstances, select an option from the remember password list box.

- **Remember password for any access**: saves the password for use with all immediate and automated operations.

- **Remember password for scripted access** (default): saves the password for use with automated operations only. For example, if the Backup Set is the destination for an overnight backup script, Retrospect will not require the password to be entered manually.

- **Do not remember password for any access**: requires you to enter the password to access the Backup Set in any way. For example, you cannot back up to it or view its properties without entering the password. After you enter the password once, you do not have to enter it again until you quit and restart Retrospect.

NOTE: You *can* change the remember password setting at a later time by modifying the Backup Set's properties. See "Configuring Backup Sets" on page 255 for more information.

Recycling Options for Tape Drive Backups

If you are backing up to tape Backup Sets, you can tell Retrospect to "recycle" the destination Backup Sets before backing up to them. Recycling enables you to reuse the tapes in a Backup Set, however all data on those tapes is lost.

WARNING: Before recycling tape Backup Sets make sure the data on its tapes exists elsewhere or that you can really afford to lose the data.
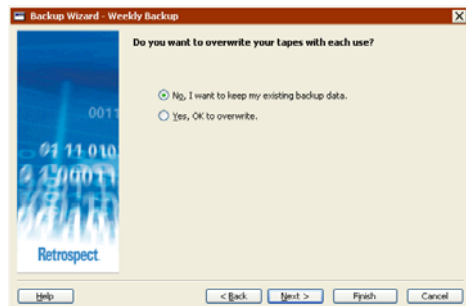
- **No, I want to keep my existing backup data**: Choose this option to preserve all existing backup data in the tape Backup Sets. Retrospect backs up only new and changed files since the last backup to each Backup Set. If the a tape member fills up, Retrospect asks for a new tape.

- **Yes, OK to overwrite**: Choose this option to recycle the tape Backup Sets before backing up. When Retrospect performs a recycle backup, it clears the Backup Sets' Catalog File contents (if any), so it appears that no files are backed up. Then it looks for the first tape member in the Backup Set and erases it if it is available. If the first member is not available, Retrospect uses any available new or erased tape. All selected files are backed up.

TIP: In Advanced Mode, you can recycle tape Backup Sets by setting the backup action for each scheduler to Recycle. See "Creating a Script Scheduler" on page 135 for more information.

Grooming Options for Hard Drive Backups

These options are only available when backing up to hard drives. The selection you make tells Retrospect what to do when the hard drive to which you are backing up becomes full (or uses all the disk space you allotted).
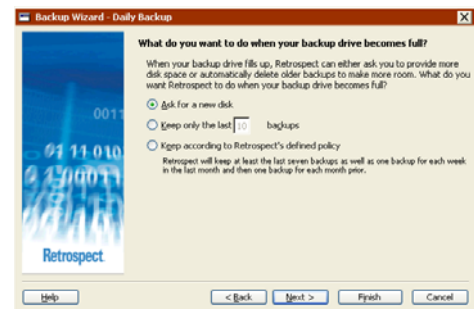

- **Ask for a new disk** When the backup drive fills up, Retrospect asks for another hard drive on which to store additional backups.

All of your backups on the original hard drive are preserved.

• **Keep only the last *n* backups**: Specify the number of backups you want to preserve when the backup drive fills up. Retrospect then automatically "grooms" (i.e., deletes) all the other, older backups on the hard drive to make room for new data.

• **Keep according to Retrospect's defined policy**: When the backup drive fills up, Retrospect uses its own grooming policy to delete old backups. At a minimum, Retrospect's policy retains two backups for each source. Retrospect keeps the last backup of the day for each source from the two most recent days on which each source was backed up. If the disk has enough space available, Retrospect keeps a backup of each source for every day in the last week, a backup for each week in the last month, and a backup for each previous month.

Reviewing the Backup Script Settings

The Backup Summary screen displays the back-up script settings you specified in the wizard.
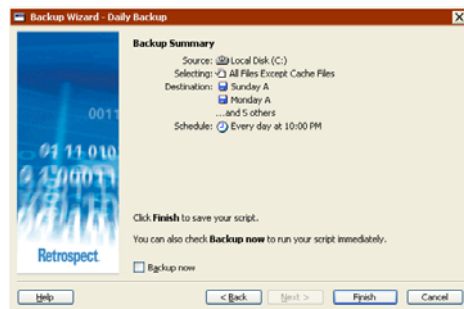
• **Source** lists the drives/folders to back up

• **Selecting** lists the file types to back up

• **Destination** lists the names of the Backup Sets to which data will be copied

• **Schedule** lists the days and time when the backup script will run

NOTE: Some options specified in the wizard are not listed in the summary screen (e.g., compression), but they are implemented during backup.

To change any of the backup script settings, click Back.

To save the script settings, click Finish. If you want to save the script settings and run the script immediately, select the Backup now check box and click Finish.

NOTE: If you select Backup now and the script includes multiple destination Backup Sets, use the drop-down menu to specify which one to use.

Editing the Backup Script Settings

To edit a backup script, choose Automate> Manage Scripts from the navigation bar. In the Scripts window, select the script you want to edit and click Edit.
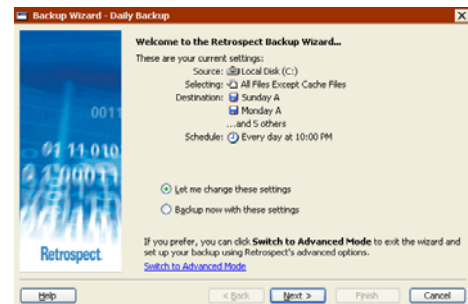
TIP: If the Advanced Mode Backup Summary screen displays, click Switch to Wizard Mode.

To edit the settings, select "Let me change these settings" and click Next. Editing the settings in Wizard Mode is much the same as creating them the first time. See "Creating a Backup Script in Wizard Mode" on page 99 for more information.

To back up now using the script settings, select "Backup now with these settings", then click Start Now.

NOTE: If the script includes multiple destination Backup Sets, use the drop-down menu to specify which one to use.

To edit the settings in Advanced Mode, click "Switch to Advanced Mode". See "Switching from Wizard to Advanced Mode" for more information.

Switching from Wizard to Advanced Mode

To access to advanced options that are not available in Wizard Mode, click "Switch to Advanced Mode" from the Welcome screen.

If you have not previously set up a backup script, you can proceed as described in "Creating a Backup Script in Advanced Mode" on page 107.

If you have previously set up a backup script, Retrospect remembers your settings and displays them in the Advanced Mode summary window.

NOTE: *All* of the Wizard Mode options are available in Advanced Mode. If you switch from Wizard to Advanced Mode, those options are mapped directly to equivalent options.

Creating a Backup Script in Advanced Mode

Creating a backup script in Advanced Mode provides access to some powerful Retrospect options that are not available in Wizard Mode. In Advanced Mode you can:

- Access more built-in selectors
- Create and apply custom selectors
- Create multiple custom schedules that include different backup actions
- Set many additional options not available in Wizard Mode

This section takes you through the steps of defining a backup script:

- Creating a Backup Script

- Setting the Backup Source
- Setting the Backup Destination
- Selecting Files to Back Up
- Setting Backup Execution Options
- Setting the Execution Unit
- Editing the Backup Script Settings

The steps for scheduling and saving are the same for all scripts:

- See "Scheduling Scripts" on page 134.
- See "Saving Scripts" on page 137.

Creating a Backup Script

1. From the navigation bar, click Automate, then click the Manage Scripts button.

The script editing window displays.
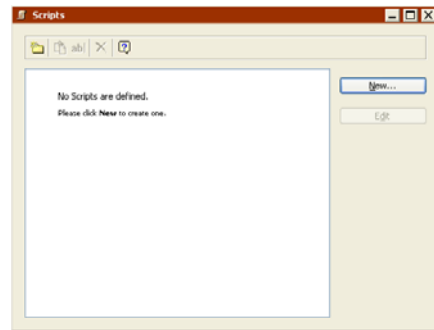
2. Click the New button to create a new script.

The script selection window displays.
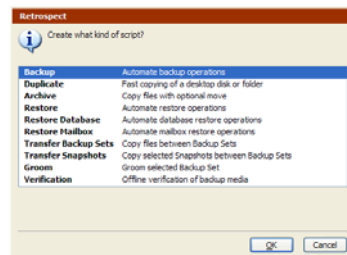
3. Select Backup from the list and click OK.

The script naming window displays.

4. Enter a name and click OK.

The script appears in its own window.
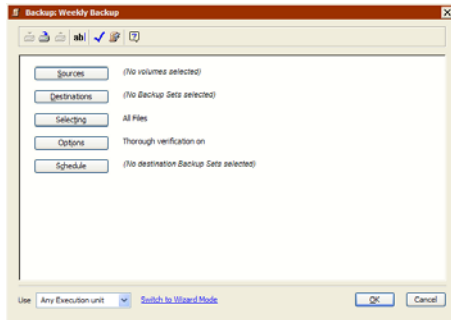
TIP: If the Retrospect Backup Wizard displays, click Switch to Advanced Mode.

This script window is very similar to the immediate backup summary window, with information for the source volumes, destination Backup Sets, file selection criteria, and options. Since this is a script, it also includes schedule information.

5. To change information, click the appropriate button.

Sources lets you add or remove source volumes.

Destinations lets you choose one or more destination Backup Sets.

Selecting lets you choose a selector—a kind of filter for selecting files and folders to be backed up.

Options displays the options window in which you can toggle verification and data compression.

Schedule lets you set the script to run at a specific time or at regular intervals.

Setting the Backup Source

The first step in defining a script is setting the source.

1. Click the Sources button.

The Source Selection window displays.
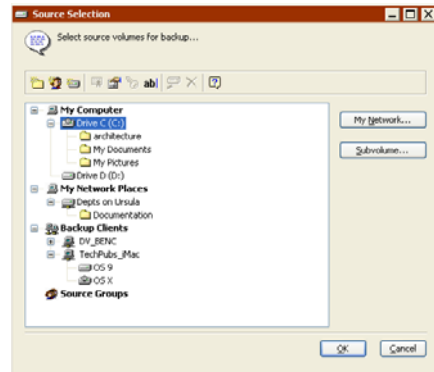
2. Select a source volume (or volumes), then click OK.
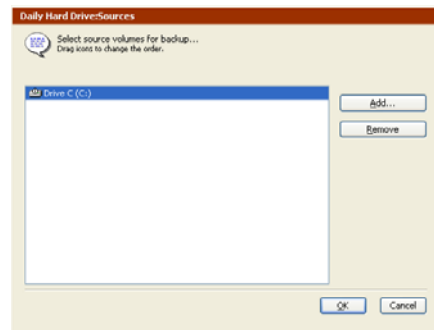
3. Click Add to select additional sources, or select a source and click Remove to remove it from the list. When the list of sources is complete, click OK.

NOTE: If there are multiple sources, they are backed up in the order listed. Click and drag to rearrange the list order.

Setting the Backup Destination

After specifying the source(s) to back up, you must specify the destination Backup Set(s) for the data.

1. Click the Destinations button.

If there are no Backup Sets defined, the Backup Set Creation Wizard launches. Create a new Backup Set, as described in "Creating Backup Sets" on page 252. The new Backup Set appears in the Backup Set Selection window.

If there are Backup Sets defined, the Backup Set Selection window displays.

You can click More or Create New to access additional Backup Sets or create new ones.

2. Select one or more Backup Sets, then click OK.

3. Click Add to select additional destinations, or select a Backup Set and click Remove to remove it from the list. When the list of destinations is complete, click OK.

Selecting Files to Back Up

By default, Retrospect selects all files except cache files on the source(s). You can choose a different pre-defined selector or create a custom selector to select a subset of files.

1. Click the Selecting button.

2. Click a selector, then click OK.

You can also click More Choices to use Retrospect's file selection criteria to create a custom selector. Selectors are explained in

detail in "Using Selectors," which starts on page 291.

NOTE: Selectors are used to determine which files are *considered* for backup, not which files actually get copied. For example, if you choose All Files, Retrospect compares all the source files with the files already in the destination Backup Set, then copies *only* those files that are new or changed.

Setting Backup Execution Options

Click the Options button to display the options window in which you can toggle verification, data compression, and other options which are explained in detail in "Execution Options," which starts on page 236.

Setting the Execution Unit

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this operation (or choose "Any Execution unit"). Make your selection in the summary window's list box. See "Assigning Execution Units" on page 162 for more information.

Editing the Backup Script Settings

To edit a backup script, choose Automate> Manage Scripts from the navigation bar. In the Scripts window, select the script you want to edit and click Edit.

NOTE: If Retrospect displays the script settings in Wizard Mode, click Switch to

Advanced Mode to display the settings in Advanced Mode.

To edit the settings, click the buttons to change the sources, destinations, file selection criteria, options, and schedule. Editing the settings in Advanced Mode is the same as creating them the first time. See "Creating a Backup Script in Advanced Mode" on page 107 for more information.

To edit the settings in Wizard Mode, click "Switch to Wizard Mode". See "Switching from Advanced to Wizard Mode" for more information.

Switching from Advanced to Wizard Mode

In general, Tqzkq recommends editing backup scripts in the same mode you created them. Of course, you can switch between the modes and if you do, it's important to know how Retrospect handles advanced options that are not available in Wizard Mode.

To return to Wizard Mode at any time, click "Switch to Wizard Mode" from the Advanced Mode summary window.

If you have made any changes to your backup script settings, Retrospect asks if you want to save those changes before switching modes.
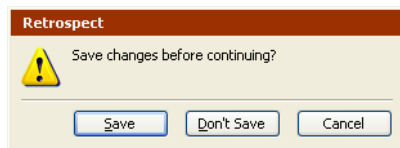
If you have not made any changes, Retrospect displays the Wizard Mode Welcome screen with a summary of the current settings.

Since Advanced Mode includes options not available in Wizard Mode, Retrospect must either keep those settings, or discard them. There are a few important options to consider:

- Selectors
- Execution Options
- Backup Sets
- Schedules
- Execution Unit

Selectors

Advanced Mode includes a number of built-in selectors that are not available in Wizard Mode. In addition, you can create and use custom selectors in Advanced Mode.

If you choose a selector that is not available in Wizard Mode, then click "Switch to Wizard Mode", Retrospect *keeps* the advanced selector and applies it when the backup script runs.

In these situations, the Wizard Mode Welcome screen displays *(Created in Advanced Mode)* in the Selecting field.

In addition, if you edit your backup settings, a new option appears in the "What type of files do you want to back up?" screen.
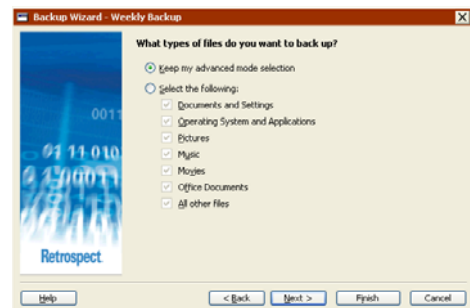
- Choose "Keep my advanced mode selection" to keep your advanced selector.
- Choose "Select the following" and select a new option to discard the advanced selector and use a new one.

Execution Options

Advanced Mode includes many execution options that are not available in Wizard Mode.

NOTE: The compression execution option is available in both Wizard and Advanced Mode. If you change the option in one mode, it will be reflected in the other.

If you choose an execution option that is not available in Wizard Mode, then click "Switch to Wizard Mode", Retrospect *keeps* the advanced execution option and applies it when the backup script runs.

WARNING: The Wizard Mode Welcome screen does not indicate whether the backup script includes advanced execution options or not. The only way to check is to switch to Advanced Mode and review the Options settings.

Backup Sets

In Advanced Mode, you can choose a file Backup Set as a destination. File Backup Sets are not available from Wizard Mode.

TIP: File Backup Sets are most useful for backing up a single file, otherwise, disk Backup Sets offer many more benefits.

If you choose a file Backup Set as a destination, then click "Switch to Wizard Mode", Retrospect *discards* the entire destination selection.

In these situations, the Wizard Mode Welcome screen displays *(No destination selected)* in the Destination field.

If you click Next, the wizard discards the destination and forces you to select a new one. Click "Switch to Advanced Mode" to continue using a file Backup Set as the destination.

Advanced Mode also allows you to select destination Backup Sets of different types. For example, the destination could be a tape Backup Set and a CD/DVD Backup Set. In Wizard Mode, all destination Backup Sets must be of the same type.

If you choose Backup Sets of different types as the destination, then click "Switch to Wizard Mode", Retrospect discards all the destination backup Sets except the first one.
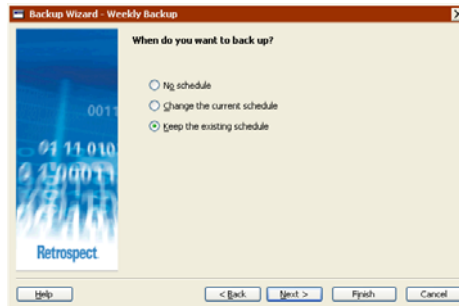
Schedules

Advanced mode includes scheduling options that are not available in Wizard mode. For example, you can create different types of schedules, create multiple schedules for a single script, and specify a backup action for a schedule. See "Scheduling Scripts" on page 134 for more information.

If you specify scheduling options that are not available in Wizard Mode, then click "Switch to Wizard Mode", Retrospect *keeps* the advanced schedule.

In these situations, the Wizard Mode Welcome screen displays *(Created in Advanced Mode)* in the Schedule field and includes a message saying the schedule cannot be edited in Wizard Mode.

In addition, if you edit your backup settings, a new option appears in the "When do you want to back up?" screen.

- Choose "Keep the existing schedule" to keep your advanced schedule.
- Choose "No schedule" to discard the advanced schedule set up an unscheduled script.
- Choose "Change the current schedule" to discard the advanced schedule and set up a new one.

Execution Unit

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for a backup script in Advanced Mode only.

If you choose a specific execution unit (not "Any Execution unit"), then click "Switch to Wizard Mode", Retrospect *keeps* the execution unit information and uses the specific execution unit when the backup script runs.

NOTE: The Wizard Mode Welcome screen does not indicate whether the script specifies an execution unit or not. The only way to check is to switch to Advanced Mode and review the settings.

SCRIPTED DUPLICATE

Duplicate scripts are great for unattended copying of hard disks, folders, or files from one volume to another. For example, you could use a duplicate script to automatically copy a local folder to a shared file server at the end of every week.

There are two ways to set up a scripted duplicate using the Manage Scripts command. You can use Retrospect's Duplicate Wizard, which walks you through the process of setting up a scripted duplicate, or you can set up the duplicate on your own in Advanced Mode. Advanced Mode has options that are unavailable in the Wizard. For more information see:

- Creating a Duplicate Script in Wizard Mode
- Switching from Wizard to Advanced Mode
- Creating a Duplicate Script in Advanced Mode
- Switching from Advanced to Wizard Mode

Creating a Duplicate Script in Wizard Mode

The Duplicate Wizard provides an easy way to set up and edit scripted duplicate operations. To start the Duplicate Wizard, click Automate from the navigation bar, then click the Manage Scripts button. The script editing window displays.

Click the New button to create a new script. The script selection window displays.
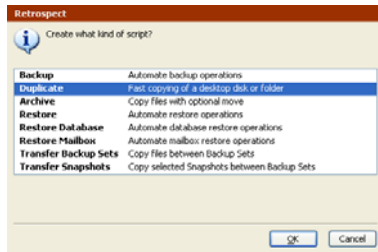
Select Duplicate from the list and click OK. In the script naming window, enter a name and click OK. The Duplicate Wizard welcome screen displays.

NOTE: If the Advanced Mode Duplicate Script summary screen displays, click Switch to Wizard Mode.
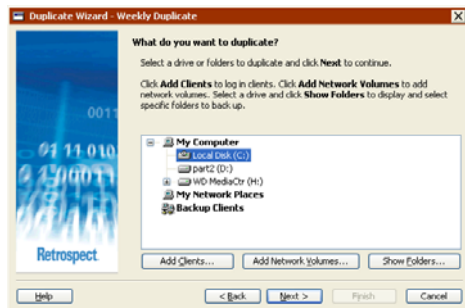
Welcome Screen

If this is the first time you are setting up a scripted duplicate, click Next to continue set up using the Duplicate Wizard. To set up the duplicate in Advanced Mode, click Switch to Advanced Mode. See "Creating a Duplicate Script in Advanced Mode" on page 116 for more information.

If you have previously set up a scripted duplicate, the welcome screen displays your current settings. See "Editing the Duplicate Script Settings" on page 115 for more information.

Choosing What to Duplicate

Select a specific drive or folder to duplicate.

Click a drive or folder to select it. This deselects any other selected drive or folder.

You can select a drive or folder from any of the containers listed in this screen: My Computer, My Network Places, or Backup Clients.

- To add Retrospect Clients to the Backup Clients container, click Add Clients.
- To add network volumes to the My Network Places container, click Add Network Volumes.
- To display the folders on a drive, select the drive and click Show Folders.

See "Containers" on page 281 for more information.

Choosing File Types to Duplicate

Select the check box for each type of file you want to duplicate. If you select all the check boxes, all files (except cache files) will be duplicated.

NOTE: Some of these options function differently with Windows, Mac OS, NetWare, and UNIX computers. The descriptions below focus on how these options interact with Windows computers. To learn how these options work with other operating systems, see "Built-in Selectors" on page 292.

- **Documents and Settings** duplicates files in the Documents and Settings folder, which contains every user's My Documents,

Favorites, Application Data, and Desktop folders.

NOTE: For Windows 9x systems, the "Documents and Settings" duplicates the "Profiles" folder.

• **Operating System and Applications** duplicates system files, including the Windows folder and the System State. Also duplicates application files, including everything in the Program Files folder, as well as files with known application extensions (like .exe and .dll) anywhere on the source.

NOTE: If you choose not to duplicate "Operating System and Applications", Retrospect modifies some of its default execution options. Retrospect turns off both the "Duplicate System State" and "Duplicate folder security information for workstations" options. See "Windows System Options" on page 244 and "Windows Security Options" on page 245 for more information.

• **Pictures** duplicates all files in the My Documents\My Pictures folder for all users. It also duplicates files with common picture file extensions (.jpg, for example) anywhere on the source, except the Windows and Program Files folders.

• **Music** duplicates all files in the My Documents\My Music folder for all users. It also duplicates files with common music file extensions (.wma and .mp3, for example) anywhere on the source, except the Windows and Program Files folders.

• **Movies** duplicates all files in the My Documents\My Videos folder for all users. It also duplicates files with common movie file extensions (.mov, for example) anywhere on the source, except the Windows and Program Files folders.

• **Office Documents** duplicates Microsoft Office Documents, Microsoft Outlook data, and Adobe PDF files anywhere on the source, except the Windows and Program Files folders.

• **All Other Files**, duplicates all files not selected by the other options.

NOTE: The Documents and Settings and Operating System and Applications options are not available if you are duplicating a folder.

Choosing the Destination

Select a drive or folder to which you want files duplicated.

NOTE: The destination cannot be the same drive or folder from which files are being duplicated. You *can* duplicate to different folders on the same drive or folders with the same names on different drives.

The Add Clients, Add Network Volumes, and Show Folders buttons on this screen function the same way as in the "What do you want to duplicate?" screen. See "Choosing What to Duplicate" on page 113.

When you click Next, Retrospect displays a dialog warning that the destination folder or drive will be completely replaced with the files you selected to duplicate.
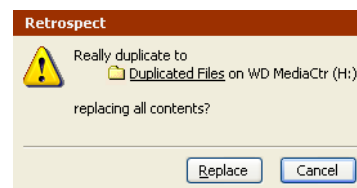
WARNING: Make sure that the destination does not contain any important files before duplicating. Any files already on the destination will be lost and replaced with the files you selected to duplicate. To be safe, create a new folder on the destination drive and duplicate to it.

Click Replace to dismiss the warning and continue setting up the duplicate script.

Choosing Whether to Create A Schedule

You can either create a script with a schedule or without a schedule.

If you choose not to create a schedule, you can still run the script manually at any time. See "Manual Script Execution" on page 139 for more information. You can also add a schedule to the script later.

Make a selection and click Next.

NOTE: If you are editing a script that already has a schedule, an additional option, "Keep the existing schedule", is also available.

Choosing When to Duplicate

Select the check box for each day you want the duplicate script to run and specify a time for the script to start.
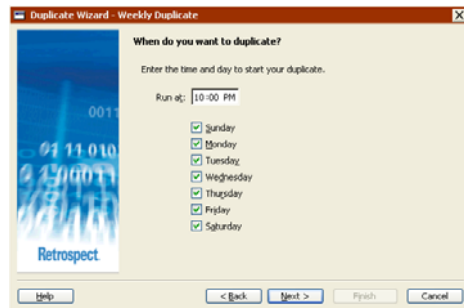
TIP: Although Retrospect can duplicate computers while they are in use, it is a good idea to run scripts after normal business hours when computers tend to be less busy.

Reviewing the Duplicate Settings

The Duplicate Summary screen displays the duplicate script settings you specified in the wizard.
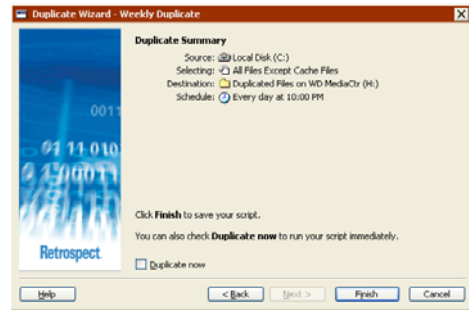
- **Source** lists the drive or folder to duplicate
- **Selecting** lists the file types to duplicate
- **Destination** lists the name of the drive or folder to which data will be copied
- **Schedule** lists the days and time when the duplicate script will run

To change any of the duplicate script settings, click Back.

To save the script settings, click Finish. If you want to save the script settings and run the script immediately, select the Duplicate now check box and click Finish.

WARNING: Duplicating can delete files on the destination. Any files already on the destination will be lost and replaced with the files you selected to duplicate. Make sure the destination does not contain important files before duplicating.

Editing the Duplicate Script Settings

To edit a duplicate script, choose Automate> Manage Scripts from the navigation bar. In the Scripts window, select the script you want to edit and click Edit.

TIP: If Retrospect displays the script settings in Advanced Mode, click Switch to Wizard Mode to display the settings in Wizard Mode.

To edit the settings, select "Let me change these settings" and click Next. Editing the settings in Wizard Mode is much the same as creating them the first time. See "Creating a Duplicate

Script in Wizard Mode" on page 112 for more information.

To duplicate now using the script settings, select "Duplicate now with these settings", then click Start Now.

To edit the settings in Advanced Mode, click "Switch to Advanced Mode". See "Switching from Wizard to Advanced Mode" for more information.

Switching from Wizard to Advanced Mode

To access advanced options that are not available in Wizard Mode, click "Switch to Advanced Mode" from the Welcome screen.

If you have not previously set up a duplicate script, you can proceed as described in "Creating a Duplicate Script in Advanced Mode" on page 116.

If you have previously set up a duplicate script, Retrospect remembers your settings and displays them in the Advanced Mode summary window.

NOTE: *All* of the Wizard Mode options are available in Advanced Mode. If you switch from Wizard to Advanced Mode, those options are mapped directly to equivalent options.

Creating a Duplicate Script in Advanced Mode

Creating a duplicate script in Advanced Mode provides access to some powerful Retrospect options that are not available in Wizard Mode. In Advanced Mode you can:

• Access more built-in selectors
• Create and apply custom selectors
• Choose a duplicate method
• Create multiple custom schedules
• Set many additional options not available in Wizard Mode

This section takes you through the steps of defining a duplicate script:

• Creating a Duplicate Script
• Setting the Duplicate Source
• Setting the Duplicate Destination
• Selecting Files to Duplicate
• Setting Duplicate Execution Options
• Setting the Execution Unit
• Editing the Duplicate Script Settings

The steps for scheduling and saving are the same for all scripts:

• See "Scheduling Scripts" on page 134.
• See "Saving Scripts" on page 137.

Creating a Duplicate Script

1. From the navigation bar, click Automate then click the Manage Scripts button.

The script editing window displays.

2. Click the New button to create a new script.

The script selection window displays.

3. Select Duplicate from the list and click OK.

The script naming window displays.

4. Enter a name and click New.

The script appears in its own window.
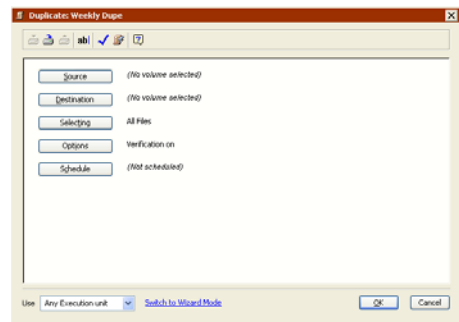
TIP: If the Retrospect Duplicate Wizard displays, click Switch to Advanced Mode.

This script window is very similar to the immediate duplicate summary window, with information for the source volume, destination

volume, file selection criteria, and options. Since this is a script, it also includes schedule information.

5. To change information, click the appropriate button.

Source lets you select a source volume.

Destination lets you select a destination volume.

Selecting lets you choose a selector, a kind of filter for selecting files and folders to be backed up.

**Options** displays the options window in which you can toggle verification, data compression, and other options.

Schedule lets you set the script to run at a specific time or at regular intervals.

Setting the Duplicate Source

Because this is a new script, Retrospect says "No volume selected" for the source.

1. Click the Source button.

The Source Selection window displays.
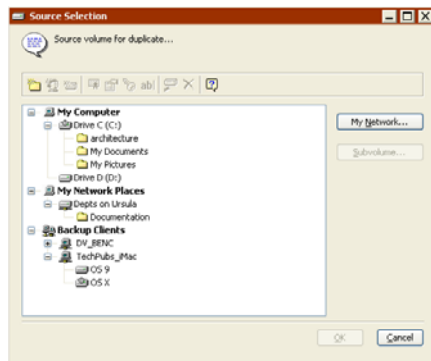
2. Select the source volume and click OK.

For details on using the volume selection window, see "Working with Volumes," which starts on page 280.

Setting the Duplicate Destination

For duplicate operations, the destination is not a Backup Set, but a volume (other than the source volume).

1. Click the Destination button.

The volume selection window displays.
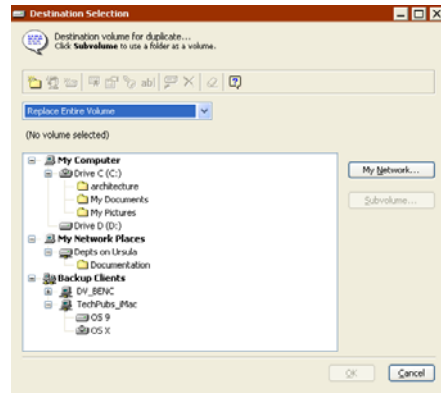
2. Select the destination volume to which you want the files copied.

3. Make a selection from the list box to specify a duplicate method (i.e., what happens to the existing contents of the destination drive).

Replace Entire Volume *replaces the entire contents* of the destination volume with the selected files and folders from the source volume. Identical files already present on the destination are not duplicated. This is the default option.

Replace Corresponding Files copies the selected files and folders to the destination volume. When Retrospect finds a file that exists on both the source and destination, the destination file is *always* overwritten. Retrospect leaves files untouched if they are identical to files marked for duplication or if the file names and locations do not match those marked.

Replace if Source is Newer copies the selected files and folders to the destination volume. When Retrospect finds a file that exists on both

the source and destination, the destination file is overwritten *only if the source file is newer*. Retrospect leaves files untouched if they are identical to files marked for duplication or if the file names and locations do not match those marked.

Duplicate Missing Files Only, copies only the selected files and folders that don't already exist on the destination volume. Other files and folders on the destination are left untouched.

WARNING: Duplicate operations can replace or delete files on the destination volume Make sure you are not overwriting or deleting important files before continuing.

4. Click OK to accept your destination choices.

Selecting Files to Duplicate

By default, Retrospect selects all files except cache files on the source. You can choose a different pre-defined selector or create a custom selector to select a subset of files.

1. Click the Selecting button.

2. Click a selector, then click OK.

You can also click More Choices to use Retrospect's file selection criteria to create a custom selector. Selectors are explained in detail in "Using Selectors," which starts on page 291.

NOTE: Selectors are used to determine which files are *considered* for duplication, not which files actually get copied. For example, if you choose All Files, Retrospect compares all the files on the source volume with the files already on the destination volume. Matching files are not copied from the source volume to the destination volume.

Setting Duplicate Execution Options

Click the Options button to display the options window in which you can set the verification, update backup report, and other options which are explained in detail in "Execution Options," which starts on page 236. One such option is to

move—rather than just copy—files from the source to the destination.

Setting the Execution Unit

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this operation (or choose "Any Execution unit'). Make your selection in the summary window's list box. See "Assigning Execution Units" on page 162 for more information.

Editing the Duplicate Script Settings

To edit a duplicate script, choose Automate> Manage Scripts from the navigation bar. In the Scripts window, select the script you want to edit and click Edit.

NOTE: If Retrospect displays the script settings in Wizard Mode, click Switch to Advanced Mode to display the settings in Advanced Mode.

To edit the settings, click the buttons to change the source, destination, file selection criteria, options, and schedule. Editing the settings in Advanced Mode is the same as creating them the first time. See "Creating a Duplicate Script in Advanced Mode" on page 116 for more information.

To edit the settings in Wizard Mode, click "Switch to Wizard Mode". See "Switching from Advanced to Wizard Mode" for more information.

Switching from Advanced to Wizard Mode

In general, Tqzkq recommends editing duplicate scripts in the same mode you created them. Of course, you can switch between the modes and if you do, it's important to know how Retrospect handles advanced options that are not available in Wizard Mode.

To return to Wizard Mode at any time, click "Switch to Wizard Mode" from the Advanced Mode summary window.

If you have made any changes to your duplicate script, Retrospect asks if you want to save those changes before switching modes.
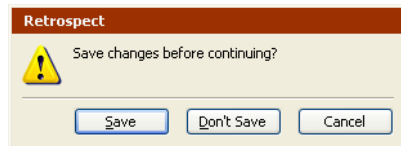
If you have not made any changes, Retrospect displays the Wizard Mode Welcome screen with a summary of the current duplicate script settings.

Since Advanced Mode includes options not available in Wizard Mode, Retrospect must either keep those settings, or discard them. There are a few important options to consider:

- Duplicate Method
- Selectors
- Execution Options
- Schedules
- Execution Unit

Duplicate Method

When choosing the destination in Advanced Mode, Retrospect lets you specify the method by which files are copied. You can choose:

- Replace Entire Volume
- Replace Corresponding Files

- Replace if Source is Newer
- Duplicate Missing Files Only

You cannot specify a duplicate method in Wizard Mode; it always uses the Replace Entire Volume method.

For more information on the difference between the duplicate methods, see "Setting the Duplicate Destination" on page 117.

Selectors

Advanced Mode includes a number of built-in selectors that are not available in Wizard Mode. In addition, you can create and use custom selectors in Advanced Mode.

If you choose a selector that is not available in Wizard Mode, then click "Switch to Wizard Mode", Retrospect *keeps* the advanced selector and applies it when you run the duplicate.

In these situations, the Wizard Mode Welcome screen displays *(Created in Advanced Mode)* in the Selecting field.
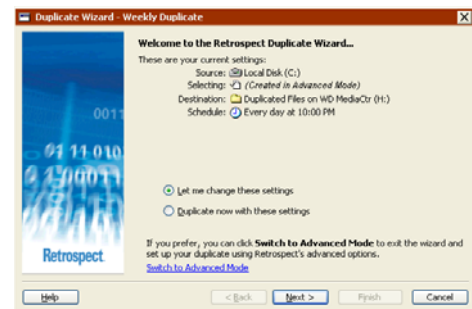
In addition, if you edit your duplicate settings, a new option appears in the "What types of files do you want to duplicate?" screen.

- Choose "Keep my advanced mode selection" to keep your advanced selector.
- Choose "Select the following" and select a new option to discard the advanced selector and use a new one.

Execution Options

Advanced Mode includes many execution options that are not available in Wizard Mode, such as verification.

If you choose an execution option that is not available in Wizard Mode, then click "Switch to Wizard Mode", Retrospect *keeps* the advanced execution option and applies it when you run the duplicate.

WARNING: The Wizard Mode Welcome screen does not indicate whether the duplicate includes advanced execution options or not. The only way to check is to switch to Advanced Mode and review the Options settings.

Schedules

Advanced mode includes scheduling options that are not available in Wizard mode. For example, you can create different types of schedules and create multiple schedules for a single script. See "Scheduling Scripts" on page 134 for more information.

If you specify scheduling options that are not available in Wizard Mode, then click "Switch to Wizard Mode", Retrospect *keeps* the advanced schedule.

In these situations, the Wizard Mode Welcome screen displays *(Created in Advanced Mode)* in the Schedule field and includes a message saying the schedule cannot be edited in Wizard Mode.

In addition, if you edit your duplicate script settings, a new option appears in the "When do you want to run the duplicate?" screen.
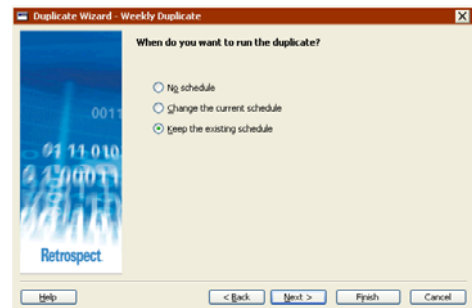
- Choose "Keep the existing schedule" to keep your advanced schedule.
- Choose "No schedule" to discard the advanced schedule set up an unscheduled script.
- Choose "Change the current schedule" to discard the advanced schedule and set up a new one.

Execution Unit

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for a duplicate script in Advanced Mode only.

If you choose a specific execution unit (not "Any Execution unit"), then click "Switch to Wizard Mode", Retrospect *keeps* the execution unit information and uses the specific execution unit when the duplicate script runs.

NOTE: The Wizard Mode Welcome screen does not indicate whether the duplicate script specifies an execution unit or not. The only way to check is to switch to Advanced Mode and review the settings.

SCRIPTED ARCHIVE

Archiving allows you to remove seldom-used files from a hard disk while maintaining a copy of those files on your storage media.

The process of creating and using an archive script is almost identical to that of a backup script.

See "Creating a Backup Script in Advanced Mode," which starts on page 107, for more information.

This section explains the differences between an archive script and a backup script.

An archive script is just like a backup script, with three main differences:

- Backup scripts support multiple destination Backup Sets, while archive scripts support a single destination Backup Set.
- Archive scripts have an additional option not available for backup scripts. For archive scripts, you can choose to move—rather than just copy—files from the source to the destination. See page 238 for details on the Move Files option.
- Archive scripts, by default, copy (or move) *all* selected files from the source to the destination. Backup scripts, by default, copy only those files which are not already present on the destination or have been

modified since the last time they were copied.

NOTE: In both cases, the default can be modified by changing the matching options. See "Matching Execution Options" on page 242 for more information.

Be sure to read "Archiving Tips" on page 68 for other important information about archiving.

SCRIPTED RESTORE

Usually, you don't know in advance when you're going to need to restore files, but there are some situations in which restore scripts are useful. You might want to create a restore script for use in a student computer lab environment, for example, in which the hard disks are restored from a common source every night.

The steps to define a restore script are:

- Creating a Restore Script
- Setting the Restore Source
- Setting the Restore Destination
- Selecting Files to Restore
- Setting Restore Execution Options
- Setting the Execution Unit

The steps for scheduling and saving are the same for all scripts:

- See "Scheduling Scripts" on page 134.
- See "Saving Scripts" on page 137.

Creating a Restore Script

1. From the navigation bar, click Automate then click the Manage Scripts button.

The script editing window displays.

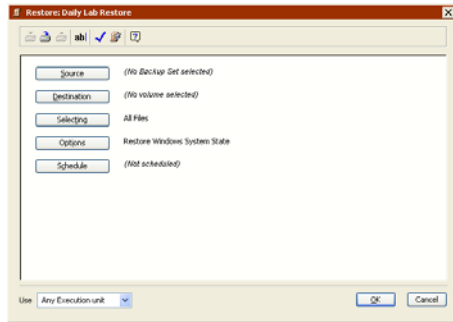**2.** Click the New button to create a new script.

The script selection window displays.

3. Select Restore from the list and click OK.

The script naming window displays.

4. Enter a name and click New.

The script appears in its own window.

This script window is very similar to the immediate restore summary window, with information for the source Backup Set, destination volume, file selection criteria, and options. Since this is a script, it also includes schedule information

5. To change information, click the appropriate button.

Source lets you specify a Backup Set and associated Snapshot from which to restore.

Destination lets you choose the destination volume.

Selecting lets you choose a selector—a kind of filter for selecting files and folders to be restored.

Options Lets you specify various options. For example, you can have Retrospect update the Date Modified information for all restored files to the current date and time.

Schedule lets you set the script to run at a specific time or at regular intervals.

Setting the Restore Source

Because this is a new script, Retrospect says "No Backup Set selected" in the script summary window.

1. Click the Source button to display a window listing Backup Sets and their Snapshots.
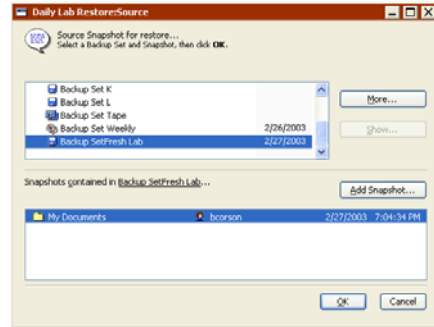
2. In the top-half of the window, select the Backup Set containing the Snapshot from which you want to restore.

NOTE: If the Backup Set you are looking for is not listed, click the More button to access additional Backup Sets by opening or recreating their Catalog Files.

3. In the bottom-half of the window, select the Snapshot.

The date and time of each Snapshot is listed.

NOTE: If the Snapshot you are looking for is not listed, click the Add Snapshot button to retrieve additional Snapshots from the storage media.

4. Click OK to continue.

The Backup Set and Snapshot date, time, and volume name are listed in the script window.

Setting the Restore Destination

Because this is a new script, Retrospect says "No volume selected" in the script window.

1. Click the Destination button.

The volume selection window displays.
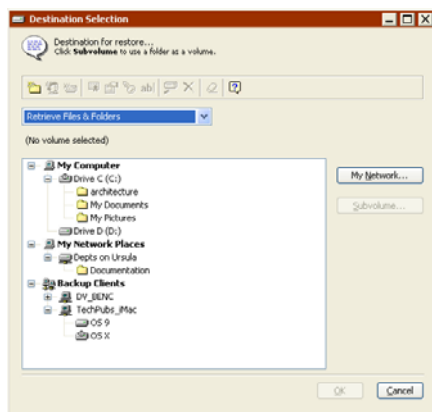
2. Select the destination volume to which you want the files restored.

3. Make a selection from the list box to specify the restore method.

Restore Entire Volume makes the destination volume exactly match the source Snapshot. It *deletes all files and folders* on the destination that do not match those marked for restore in the Snapshot, leaving files untouched if they are identical to files marked for restore. It then copies all remaining files and folders from the Snapshot to the destination, preserving the folder hierarchy. This is the default restore method if you chose "Restore an entire volume". If you select this method, Retrospect restores registry and System State information from the Snapshot (if both the Snapshot and destination are system volumes) by default.

NOTE: To prevent the operating system from crashing, the Restore Entire Volume method does not delete the active Windows system, nor does it delete the "blessed" system folder of a Mac OS client.

Replace Corresponding Files restores all selected files from the Snapshot that do not exist on the destination and overwrites files on the destination that also exist in the source Snapshot. These "corresponding" or "matching" files on the destination are *always* overwritten with files from the Snapshot

regardless of whether the Snapshot file is newer or older than the destination file. Retrospect leaves files untouched if they are identical to files marked for restore, if the file names do not match those marked for restore, or if the path to those files is not identical. If you select this method and choose the Restore System State execution option, Retrospect restores registry and System State information from the Snapshot (if both the Snapshot and destination are system volumes).

Replace if Backup is Newer restores all selected files from the Snapshot that do not exist on the destination and overwrites matching files on the destination only if the Snapshot file is newer than the destination file. If you select this method and choose the Restore System State execution option, Retrospect restores registry and System State information from the Snapshot (if both the Snapshot and destination are system volumes).

Restore Missing Files Only restores all selected files from the Snapshot that do not exist on the destination, but does not overwrite any files on the destination. Matching files on the destination are left untouched. If you select this method and choose the Restore System State execution option, Retrospect restores registry and System State information from the Snapshot (if both the Snapshot and destination are system volumes).

NOTE: To restore *just* the registry and System State, choose "Restore Missing Files Only", then click Files Chosen and make sure no files are selected, and finally click Options>More Choices and select the Restore System State check box.

Retrieve Files & Folders creates a new folder on the destination volume (giving the folder the name of the Backup Set), then copies all selected files from the Snapshot into this folder, preserving the Snapshot folder hierarchy. Nothing is replaced or overwritten. This is the default restore method if you chose "Restore

files and folders". This method never restores registry and System State information.

Retrieve Just Files creates a new folder on the destination volume (giving the folder the name of the Backup Set), then copies all selected files from the Snapshot into this folder. The Snapshot folder hierarchy is *not* preserved. Nothing is replaced or overwritten. This method never restores registry and System State information.

WARNING: The Restore Entire Volume, Replace Corresponding Files, and Replace if Backup is Newer methods may destroy data on the destination. If you choose one of these methods, be sure it is acceptable to erase or replace files on the destination volume.

4. Click OK.

Selecting Files to Restore

By default, Retrospect selects all files from the source Backup Set. You can choose a different pre-defined selector or create a custom selector to select a subset of all files.

1. Click the Selecting button.

2. Click a selector, then click OK.

You can also click More Choices to use Retrospect's file selection criteria to create a custom selector. Selectors are explained in detail in "Using Selectors," which starts on page 291.

NOTE: Selectors are used to determine which files are *considered* for restoring, not which files actually get restored. For example, if you choose All Files, Retrospect compares all the files in the source Backup Set with the files already on the destination volume. Matching files are not copied from the source to the destination.

Setting Restore Execution Options

Click the Options button to display the options window. Then, click More Choices to specify a number of options that are explained in detail in "Execution Options," which starts on page 236.

The Update modify dates option is only available for restore operations. See "Files Execution Options" on page 239 for more information.

Setting the Execution Unit

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this operation (or choose "Any Execution unit'). Make your selection in the summary window's list box. See "Assigning Execution Units" on page 162 for more information.

SCRIPTED BACKUP SET TRANSFER

If you need to copy all files and Snapshots from one or more Backup Sets to a single new or existing Backup Set on a regular basis, you can create a Transfer Backup Sets script to automate this process. These scripts can be used to:

• Clone a Backup Set

• Protect against media failure

• Provide for offsite storage

• Start a new cycle of backups

• Consolidate multiple BackupSets to a single Backup Set

Transferring Backup Sets scripts, by default, match files in the source to files already in the destination and only copy the necessary files. Existing Snapshots and files on the destination remain untouched.

Transfer Backup Sets scripts do not have a preview feature. You must rely on selectors instead of picking and choosing files by hand.

To transfer files between Backup Sets, you must have a separate tape or CD/DVD drive for each Backup Set, even if both Backup Sets are on the same type of media. In the case of disk and file

Backup Sets the need for separate backup devices does not apply.

TIP: If you do not have separate drivesfor each Backup Set, you can first transfer files temporarily to a disk Backup Set and then transfer the disk Backup Set to the final destination Backup Set.

The steps to create a Transfer Backup Sets script are:

- Creating a Transfer Backup Sets Script
- Selecting the Transfer Backup Sets Source
- Selecting the Transfer Backup Sets Destination
- Selecting Files to Transfer
- Setting Additional Options
- Setting the Execution Unit

The steps for scheduling and saving are the same for all scripts:

- See "Scheduling Scripts" on page 134.
- See "Saving Scripts" on page 137.

Creating a Transfer Backup Sets Script

1. From the navigation bar, click Automate then click the Manage Scripts button.

The script editing window displays.

2. Click the New button to create a new script.

The script selection window displays.

3. Select Transfer Backup Sets from the list and click OK.

The script naming window displays.

4. Enter a name and click New.

The script appears in its own window.
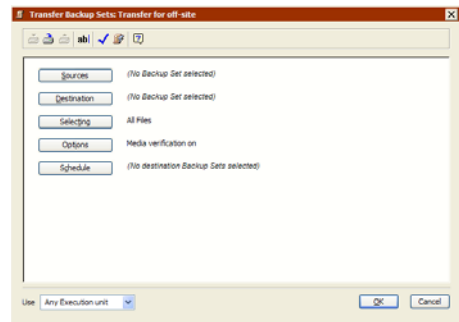
This script window is very similar to the immediate Transfer Backup Sets summary window, with information for the source Backup Set(s), destination Backup Set, file selection criteria, and options. Since this is a script, it also includes schedule information.

5. To change information, clickthe appropriate button.

Sources lets you specify one or more Backup Sets.

Destination lets you choose the destination Backup Set.

Selecting lets you choose a selector, a kind of filter for selecting files and folders to be transferred.

Options Lets you specify various options, including verification and data compression.

Schedule lets you set the script to run at a specific time or at regular intervals.

Selecting the Transfer Backup Sets Source

Because this is a new script, Retrospect says "No Backup Set selected" in the Sources section of the script summary window.

1. Click the Sources button to display the Backup Set Selection window.
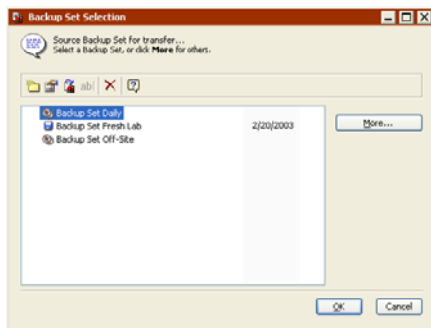
2. Select one or more Backup Sets containing the data you want to transfer.

If the Backup Set you are looking for is not listed, click the More button to access additional Backup Sets by opening or recreating their Catalog Files.

NOTE: Transfer Backup Sets scripts copy *all* Snapshots and associated files in the source Backup Set(s) to the destination Backup Set. This is different from Transfer Snapshots scripts, which copy only *active* Snapshots and associated files. See "Scripted Snapshot Transfer" on page 127 for more information.

3. Click OK.

The Backup Set(s) are listed in the script window.

Selecting the Transfer Backup Sets Destination

Because this is a new script, Retrospect says "No Backup Set selected" in the Destination section of the script window.

1. Click the Destination button.

The Backup Set Selection window displays.
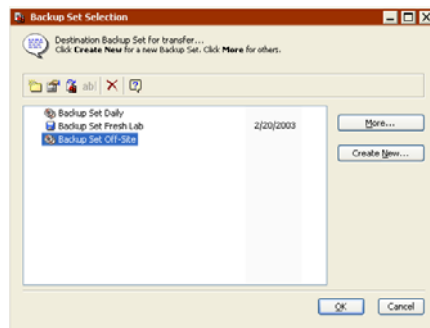
2. Select the destination Backup Set.

If the only Backup Sets listed in the window are already specified as the source, or if you do not want to use any of the Backup Sets in the list as the destination, click Create New to create a new Backup Set. See "Creating Backup Sets" on page 252 for more information.

NOTE: The destination Backup Set and the source Backup Set *must* be different.

3. Click OK.

Selecting Files to Transfer

By default, Retrospect selects all files from the source Backup Set(s). You can choose a different pre-defined selector or create a custom selector to select a subset of all files.

1. Click the Selecting button.

2. Click a selector, then click OK.

You can also click More Choices to use Retrospect's file selection criteria to create a custom selector. Selectors are explained in detail in "Using Selectors," which starts on page 291.

Setting Additional Options

Retrospect includes a number of execution options that are specific to Backup Set Transfers.

Click Options in the summary window to change the default settings for the Copy Snapshots, Verification, Data compression, Recycle source Backup Set, and other options.
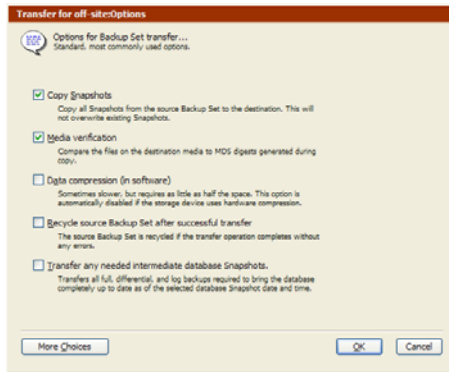
See "Transfer Execution Options" on page 239 for more information about these options.

Click the More Choices button to access additional execution options. See "Execution Options" on page 236 for more information.

Setting the Execution Unit

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this script (or choose "Any Execution unit'). Make your selection in the summary window's list box. See "Assigning Execution Units" on page 162 for more information.

SCRIPTED SNAPSHOT TRANSFER

If you need to copy Snapshots and their associated files from their source Backup Sets to a new or existing Backup Set on a regular basis, you can create a Transfer Snapshots script to automate this process. These scripts can be used to:

• Start a new Backup Set with a synthetic full backup

• Create an offsite disaster recovery Backup Set

• Start a new cycle of backups with a full backup

Transfer Snapshots scripts are different from Transfer Backup Sets scripts in a number of ways. Transfer Snapshots scripts:

• Transfer only *active* Snapshots; Transfer Backup Sets scripts transfer *all* Snapshots.

• Provide different methods for selecting which Snapshots get transferred; Transfer Backup Sets scripts always transfer *all* Snapshots.

By default, transferring Snapshots matches files in the source to files already in the destination and only copies the necessary files. Existing Snapshots and files on the destination remain untouched.

Transfer Snapshots scripts do not have a preview feature. You must rely on selectors instead of picking and choosing files by hand.

To transfer Snapshots between Backup Sets, you must have a separate tape or CD/DVD drive for each Backup Set, even if both Backup Sets are on the same type of media. In the case of disk and file Backup Sets the need for separate backup devices does not apply.

TIP: If you do not have separate drives for each Backup Set, you can first transfer Snapshots temporarily to a disk Backup Set and then transfer the disk Backup Set Snapshots to the final destination Backup Set.

Snapshot Transfer and Synthetic Fulls

Transfer Snapshots scripts allows you to create what Retrospect calls a "synthetic full" backup. Retrospect creates synthetic fulls when transferring Snapshots to:

• A new Backup Set

• An existing Backup Set when the "Match source Catalog File to destination Catalog File" option is turned off

Synthetic fulls allow you to quickly seed a new Backup Set with only the most recent Snapshots (for example) from an existing Backup Set. This

allows you to start a fresh cycle of backups without losing the time-saving benefits of Progressive Backup. Subsequent backups to the new Backup Set will copy only new and changed files.

After the transfer, the destination Backup Set contains the same data it would after a full backup. You get a full backup without having to perform the more time-consuming process of executing a *actual* full backup.

NOTE: A synthetic full backup is the equivalent of a full backup done *at the time of* the most recent Snapshots. It does not include files that are new or changed since the date and time of those Snapshots, nor does it include older versions of files contained in non-current Snapshots.

Synthetic fulls are also useful for creating a Backup Set that contains all its files in one contiguous session. This allows Retrospect to restore entire volumes more quickly, since it does not have to search through multiple sessions to find all the required files.

The steps to create a Transfer Snapshots script are:

- Creating a Transfer Snapshots Script
- Selecting the Transfer Snapshots Source
- Selecting the Transfer Snapshots Destination
- Selecting the Files to Transfer
- Setting Additional Options
- Setting the Execution Unit

The steps for scheduling and saving are the same for all scripts:

- See "Scheduling Scripts" on page 134.
- See "Saving Scripts" on page 137.

Creating a Transfer Snapshots Script

1. From the navigation bar, click Automate then click the Manage Scripts button.

The script editing window displays.

2. Click the New button to create a new script.

The script selection window displays.

3. Select Transfer Snapshots from the list and click OK.

The script naming window displays.

4. Enter a name and click New.

The script appears in its own window.
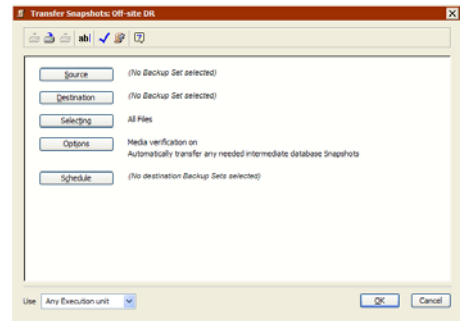
This script window is very similar to the immediate Transfer Snapshots summary window, with information for the source Backup Set, destination Backup Set, file selection criteria, and options. Since this is a script, it also includes schedule information.

5. To change information, click the appropriate button.

Source lets you specify source Backup Sets and Snapshots.

Destination lets you choose the destination Backup Set.

Selecting lets you choose a selector, a kind of filter for selecting files and folders to be transferred.

Options lets you specify various options, including verification and data compression.

Schedule lets you set the script to run at a specific time or at regular intervals.

Selecting the Transfer Snapshots Source

Because this is a new script, Retrospect says "No Backup Set selected" in the Source section of the script summary window.

1. Click the Source button to display the source window.

2. In the source selection window's top list, select the Backup Set containing the Snapshot(s) you want to transfer.

If the Backup Set you are looking for is not listed, click the More button to access additional Backup Sets by opening or recreating their Catalog Files.

Retrospect displays a list of the selected Backup Set's *active* Snapshots in the window's bottom list, along with the date and time of the Snapshot and the name of the backed up volume.

NOTE: The list of Snapshots is only displayed if you select one of the following options: "Selected Snapshots" or "The most recent Snapshot for each source selected". Only Backup Sets with a date next to them contain Snapshots.

By default, Retrospect saves the most recent Snapshot for each volume (or subvolume) that was backed up in its Catalog File. These Snapshots are considered *active*. All Snapshots, including older ones, are saved on the backup media (tape, disk, or CD/DVD). Following each successful backup or archive operation, the old Snapshot is replaced in the Catalog File with the new one. The old Snapshot remains untouched on the backup media and can be retrieved when needed.

NOTE: A disk Backup Set with grooming enabled saves all the Snapshots required by its grooming policy in the Catalog File. For example, if you told Retrospect to save the last 10 backups, then up to ten Snapshots for each volume will be active. In addition, any Snapshots that have been manually locked are also active.

3. Click Add Snapshot if the Snapshot you want to transfer is not listed.

Retrospect displays a list of all Snapshots in the Backup Set. Select a Snapshot and click Retrieve to copy the older Snapshot from the Backup Set media (which may require you to insert media) and add it to the list in the source selection window. That Snapshot is now *active*.

NOTE: The Retrieve button is disabled when you select a Snapshot that is already available.

4. Select the Snapshot(s) to transfer.

Once you select a source Backup Set, there are a number of ways to select which Snapshots to transfer.

• **The most recent Snapshot for each source** transfers the most recent Snapshot and associated files for each volume (or subvolume) in the active Snapshots list. Retrospect transfers whatever the most recent Snapshots are *at the time the script runs*.

• **The most recent Snapshot for each source selected** transfers the most recent Snapshot and associated files for each volume (or subvolume) you select in the active Snapshots list. Retrospect transfers whatever the most recent Snapshots are for

the selected sources *at the time the script runs*.

- **All active Snapshots for each source** transfers all *active* Snapshots and associated files. To see the list of active Snapshots and their sources, temporarily choose the "Selected Snapshots" option. Make sure to choose "All active Snapshots for each source" again before clicking OK. To make an older Snapshot active, click Add Snapshot.

- **Selected Snapshots** transfers only those Snapshots (and associated files) that you select from the active Snapshots list. Control-click or Shift-click to select multiple Snapshots. To make an older Snapshot active, click Add Snapshot.

"The most recent Snapshot..." options are very useful for Transfer Snapshots scripts since the list of a Backup Set's active Snapshots changes each time you back up.

NOTE: Transfer Snapshots scripts only copy active Snapshots. To copy *all* Snapshots, use a Transfer Backup Sets script. See "Scripted Backup Set Transfer" on page 124 for more information.

5. Click OK.

The Backup Set and Snapshot information is displayed in the source window.

To transfer additional Snapshots, click Add.

To remove a source, select it and click Remove.

When you are satisfied with your selections click OK.

Selecting the Transfer Snapshots Destination

Because this is a new script, Retrospect says "No Backup Set selected" in the Destination section of the script window.

1. Click the Destination button.

The Backup Set Selection window displays.
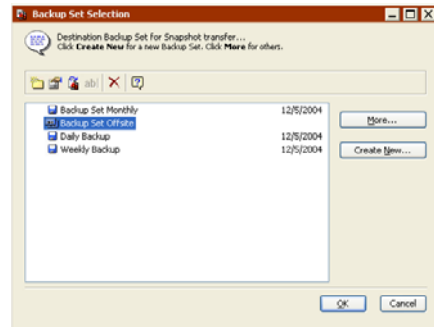
2. Select the destination Backup Set.

If you do not want to use any of the Backup Sets in the list as the destination, click Create New to create a new Backup Set. See "Creating Backup Sets" on page 252 for more information.

3. Click OK.

Selecting the Files to Transfer

By default, Retrospect transfers all files from the selected Snapshots to the destination Backup Set. You can choose a different selector to transfer a subset of all files.

1. Click the Selecting button.

2. Click a selector, then click OK.

You can also click More Choices to use Retrospect's file selection criteria to create a custom selector. Selectors are explained in detail in "Using Selectors," which starts on page 291.

Setting Additional Options

Retrospect includes a number of execution options that are specific to Snapshot transfers.

Click Options in the summary window to change the default settings for Media Verification, Data compression, Recycle source Backup Set, and other options.
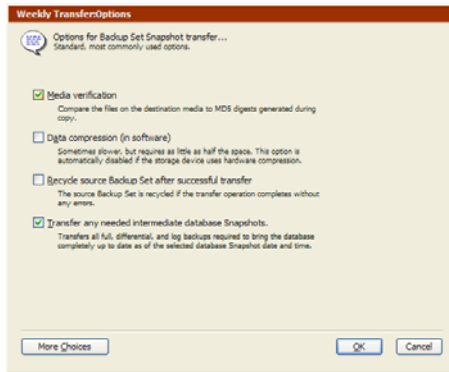
See "Transfer Execution Options" on page 239 for more information about these options.

Click the More Choices button to access additional execution options. See "Execution Options" on page 236 for more information.

Setting the Execution Unit

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this script (or choose "Any Execution unit"). Make your selection in the summary window's list box. See "Assigning Execution Units" on page 162 for more information.

SCRIPTED GROOMING

Groom scripts provide the ability to schedule a time to reclaim disk space. When a Groom script runs, Retrospect deletes older files and folders from the source disk Backup Set(s) based on its specified grooming policy. In the absence of a Groom script, Retrospect won't delete older files and folders until it requires more disk space.

NOTE: See "The Options tab" on page 256 for more information on enabling grooming for disk Backup Sets.

The steps to create a Groom script are:

   • Creating a Groom Script

   • Selecting the Source to Groom

   • Setting the Execution Unit

The steps for scheduling and saving are the same for all scripts:

   • See "Scheduling Scripts" on page 134.

   • See "Saving Scripts" on page 137.

Creating a Groom Script

1. From the navigation bar, click Automate then click the Manage Scripts button.

The script editing window displays.

2. Click the New button to create a new script.

The script selection window displays.

3. Select Groom from the list and click OK.

The script naming window displays.

4. Enter a name and click New.

The script appears in its own window.
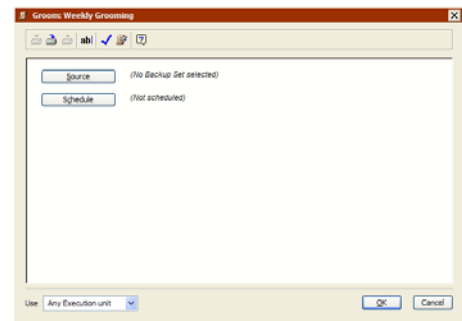
5. To add information to the script, click the appropriate button.

Source lets you specify one or more Backup Sets. See Selecting the Source to Groom.

Schedule lets you set the script to run at a specific time or at regular intervals. See Scheduling Scripts.

When the information in the script window is correct, you can save the script. See "Saving Scripts" on page 137.

Selecting the Source to Groom

If this is a new script, Retrospect says "No Backup Set selected" in the Source section of the script summary window.

1. Click the Source button to display the Backup Set Selection window.
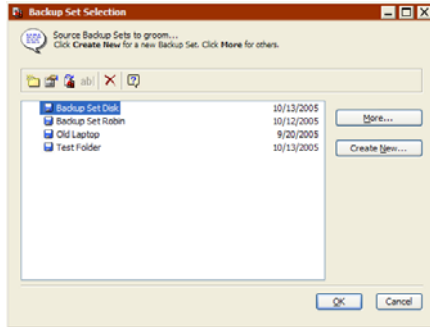

NOTE: Retrospect displays *only* disk Backup Sets, since grooming is not supported with other media types.

2. Select one or more Backup Sets containing data you want to groom.

If the Backup Set you are looking for is not listed, click the More button to access additional Backup Sets by opening or recreating their Catalog Files.

NOTE: If you select a Backup Set that does not have grooming enabled, Retrospect will report an error in the Operations Log when the script runs and then continue grooming any additional source Backup Sets.

3. Click OK.

The Backup Set(s) are listed in the script window.

Setting the Execution Unit

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this script (or choose "Any Execution unit'). Make your selection in the summary window's list box. See "Assigning Execution Units" on page 162 for more information.

SCRIPTED VERIFICATION

Verification scripts provide the ability to schedule Backup Set media verification. This "offline verification" is a useful tool for maximizing your backup window. To manually verify media, choose Tools>Verify Media from Retrospect's navigation bar. See "Verifying Backup Set Media" on page 305 for more information.

For example, if your backup script is unable to complete during the evening when users are away from their computers, you can choose "No verification" for the backup script, then schedule a separate verification script to run in the morning. Since the backup script no longer includes a verification phase, it will finish more quickly.

Whenever possible, verification scripts verify data on Backup Set media by comparing the files in the source Backup Set to MD5 digests generated during the backup. This means that Retrospect does not need to access the backed up source volumes, which prevents slowdowns on those volumes.

In certain circumstances, Retrospect does not have access to MD5 digests generated during backup. This is true for all backups created using versions of Retrospect prior to Retrospect 7.5, as well as backups that took place when Retrospect's "Generate MD5 digests during backup operations" preference was disabled. See "Verification Preferences" on page 270 for more information.

In these cases, Retrospect still checks all files on the Backup Set media to make sure that they are readable.

NOTE: Verification scripts *do* require you to reinsert media when verifying backups that span media.

The steps to create a Verification script are:

   • Creating a Verification Script
   • Selecting the Verification Source
   • Setting Additional Options
   • Setting the Execution Unit

The steps for scheduling and saving are the same for all scripts:

   • See "Scheduling Scripts" on page 134.
   • See "Saving Scripts" on page 137.

Creating a Verification Script

1. From the navigation bar, click Automate then click the Manage Scripts button.

The script editing window displays.

2. Click the New button to create a new script.

The script selection window displays.

3. Select Verification from the list and click OK.

The script naming window displays.

4. Enter a name and click New.

The script appears in its own window.
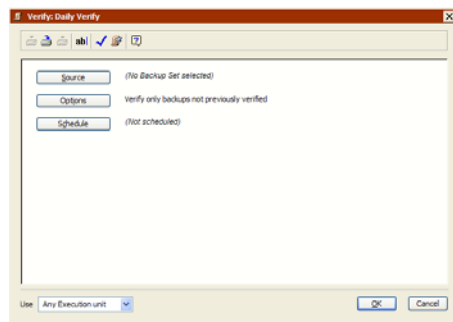
5. To add information to the script, click the appropriate button.

Source lets you specify one or more Backup Sets. See Selecting the Verification Source.

Options lets you specify the verification options. See Setting Additional Options.

Schedule lets you set the script to run at a specific time or at regular intervals. See Scheduling Scripts.

When the information in the script window is correct, you can save the script. See "Saving Scripts" on page 137.

Selecting the Verification Source

If this is a new script, Retrospect says "No Backup Set selected" in the Source section of the script summary window.

1. Click the Source button to display the Backup Set Selection window.
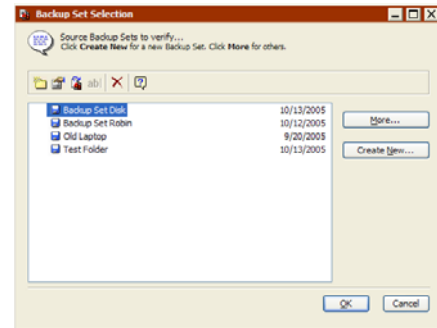
2. Select one or more Backup Sets containing data you want to verify.

If the Backup Set you are looking for is not listed, click the More button to access additional Backup Sets by opening or recreating their Catalog Files.

3. Click OK.

The Backup Set(s) are listed in the script window.

Setting Additional Options

Retrospect includes an execution option that is specific to Verification scripts.

Click Options in the summary window to change the default setting for which backups you want to verify.
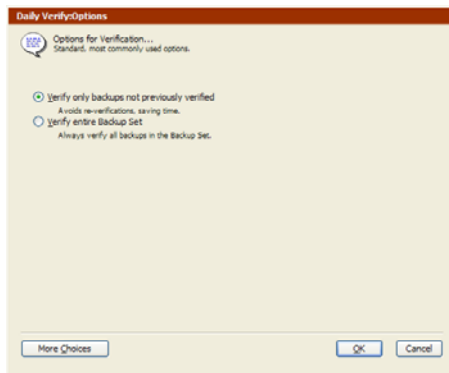
See "Verification Execution Options" on page 243 for more information about this option.

Click the More Choices button to access additional execution options. See "Execution Options" on page 236 for more information.

Setting the Execution Unit

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this script (or choose "Any Execution unit'). Make your selection in the summary window's list box. See "Assigning Execution Units" on page 162 for more information.

SCHEDULING SCRIPTS

Although you can manually execute a script at any time, scripts are designed to run unattended. In order to accomplish this, you need to create a schedule to specify when and how often to run the script.

NOTE: If you want to execute the script only upon your command and in your presence, see "Manual Script Execution," which starts on page 139.

You can schedule a script to run automatically on specified days or on a repeating schedule, such as every two weeks. You can define multiple schedules for the same script and specify the

kind of backup you want for each scheduled execution.

For more information about using scripts as part of an overall backup strategy, see "Backup Strategies" on page 224.

To schedule a script:

1. In the script summary window, click the Schedule button.

The Schedule window displays.
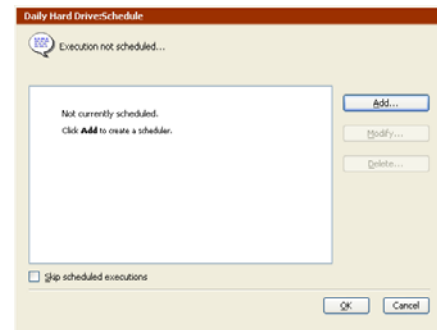
2. Click the Add button.
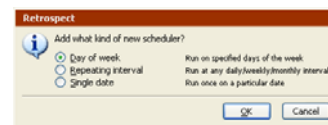
3. Specify the type of scheduler you'd like to add, then click OK.

Day of week lets you define a schedule for one or more days of the week and specify a weekly repeating interval. For example, you could schedule a script to run on Monday and Wednesday, every other week. Keep in mind that *a week starts on the Sunday of the week of the start date.*

Repeating interval lets you define a schedule that is repeated after a specified interval. For example, the last Friday of every month or every three hours.

Single date lets you define a schedule for a single date and time. For example, April 19, 2003 at 6:00 A.M.

NOTE: A script can contain any combination of one or more of these schedulers.

4. Create the scheduler as described in "Creating a Script Scheduler," which starts on page 135, then click OK.

The Schedule window displays.
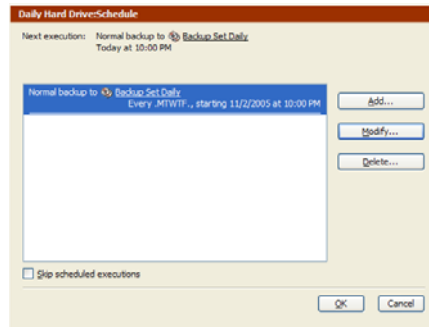
5. Click Add to create additional schedulers; click Modify to change the selected scheduler; or click Delete to remove the selected scheduler.

6. Click OK when you're done scheduling the script.

The script summary window displays.
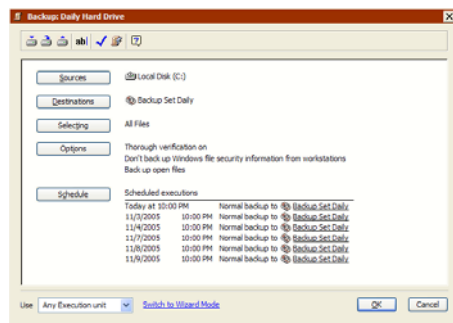
It lists the next six scheduled executions based on the scheduler(s) you created.

Creating a Script Scheduler

There are three types of schedulers available in Retrospect:

• Day of week

• Repeating interval

• Single date

While these schedulers have some common elements, the process for creating each type is somewhat unique.

Common Scheduler Elements

All scheduler types have a few common controls and settings. They are:

• Start Date and Time: This determines the earliest time at which the script is permitted to execute. To change the start date and time, click on any individual part of the date or time. When the item is selected, type the new information or click the arrows to change the information. (You can also press the up and down arrows on your keyboard. Press the Tab key to move the selection among the different elements.)

• Backup Action Type and Destination: If you are creating a scheduler for a backup script, you can also specify a backup action and destination. From the Action list box, choose Normal, New Member, Recycle, or New Backup Set. (backup and transfer scripts only)

Start Date and Time This determines the earliest time at which the script is permitted to execute. To change the start date and time, click on any individual part of the date or time. When the item is selected, type the new information or click the arrows to change the information. (You can also press the up and down arrows on your keyboard. Press the Tab key to move the selection among the different elements.)

NOTE: For Day of week schedulers, specifying a start date does not mean a script will execute on that date, or even in the same week. Check the summary at the top of the window to see the actual date the script will first execute.

Backup Action Type and Destination If you are creating a scheduler for a backup or transfer script, you can also specify a backup action. From the Action list box, choose Normal, New Member, Recycle, or New Backup Set.

- **Normal** is a typical Progressive Backup. It selects only files that are new, newly-modified, or new to the Backup Set and appends them to existing members.

- **New Member** skips to a new member of the specified Backup Set. Retrospect will use an existing member with the correct name, or any new or erased media of the correct type. New Member is just like Normal, except files are copied to the next member of the Backup Set.

- **Recycle** clears the Catalog contents (if any) of a Backup Set so it appears no files are backed up. Then it looks for the first media member of the Backup Set and erases it if it is available. If the first member is not available, Retrospect uses any available new or erased medium. Everything selected from the source is backed up to the Backup Set.

- **New Backup Set** makes a new Backup Set (with a name similar to the old one) using a new or erased medium. The original Backup Set and its Catalog remain intact for long-term storage in a safe place. The new Backup Set and its Catalog are named with a number in sequence.

Retrospect allows you to have more than one Backup Set for a script so you can rotate media as part of your backup strategy. If the script has multiple Backup Set destinations, use the To list box to choose the Backup Set to be used for the scheduled execution.

NOTE: The list box is not displayed if only one Backup Set is specified in the script.

Using the Day of Week Scheduler

If you want to run a script on specified days of the week, use a the Day of week scheduler.

To create a Day of week scheduler:

1. Select the Day of week radio button in the Scheduler dialog box.
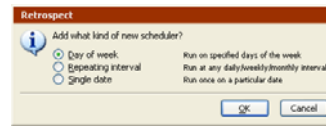
2. Click OK.

The Day of Week scheduler window displays.
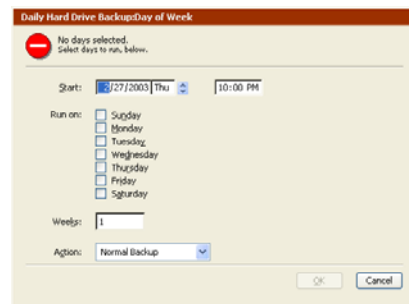
3. Set the start date and time as described in "Common Scheduler Elements" on page 135.

NOTE: Retrospect's Schedule preference (see page 264) defines the time period during which scripts are allowed to execute. Scripts scheduled to execute outside this period will not run.

If necessary specify the backup action and destination Backup Set.

4. Click the checkboxes for the days of the week you want the script to execute.

5. Enter a number to use as the repeating interval for the weeks.

For example, if you enter two, the script executes every other week (or every two weeks).

6. When all of the settings in the scheduler window are correct, click OK.

Using the Repeating Interval Scheduler

If you want a script to run at a specified hourly, daily, weekly, or monthly interval, use a Repeating interval scheduler.
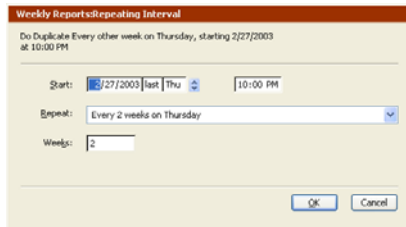
To create a Repeating interval scheduler:

1. Select the Repeating interval radio button in the Scheduler dialog box.
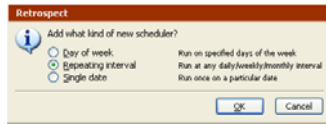
2. Click OK.

The Repeating interval scheduler window displays.

3. Set the start date and time as described in "Common Scheduler Elements" on page 135.

NOTE: Retrospect's Schedule preference (see page 264) defines the time period during which scripts are allowed to execute. Scripts scheduled to execute outside this period will not run.

If necessary specify the backup action and destination Backup Set.

4. From the Repeat list box, select the time unit (Hours, Days, Weeks, or Months) for the repeating interval.

5. Type a repeat interval in the Hours, Days, Weeks, or Months field.

The Repeat list box changes to reflect the Repeat Interval you enter.

6. When all of the settings in the scheduler window are correct, click OK.

Using the Single Date Scheduler

If you want a script to run once at a specified date and time, use the Single date scheduler.

To create a Single date scheduler:

1. Select the Single date radio button in the Scheduler dialog box.
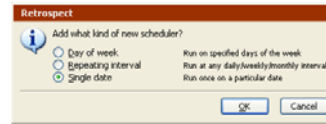
2. Click OK.

The Single date scheduler window displays.
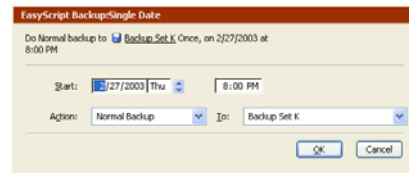
3. Set the start date and time as described in "Common Scheduler Elements" on page 135.

NOTE: Retrospect's Schedule preference (see page 264) defines the time period during which scripts are allowed to execute. Scripts scheduled to execute outside this period will not run.

If necessary specify the backup action and destination Backup Set.

4. When all of the settings in the scheduler window are correct, click OK.

SAVING SCRIPTS

After you've specified all the script settings, you need to save the script. There are three options for saving:

- Save: Click the Save icon to save the script using the name you created it with. You can also just click the OK button in the script summary window.

- Save As: Click the Save As icon to save the script using a new name. You can save a script once, modify the settings, then Save As to create a new script.

• Save and Run: Click the Save and Run icon ![icon] to save the script and display the Manual Script Execution window. You can then choose to execute the script immediately, or create a "run document".

For more information on executing saved scripts, see "Executing Scripts," which starts on page 139.

Scheduled Operations

Retrospect keeps track of all of your scheduled scripts and automatically executes them at the time you specified. To view a list of scheduled scripts, click Activity Monitor from Retrospect's navigation bar, then click the Scheduled button.
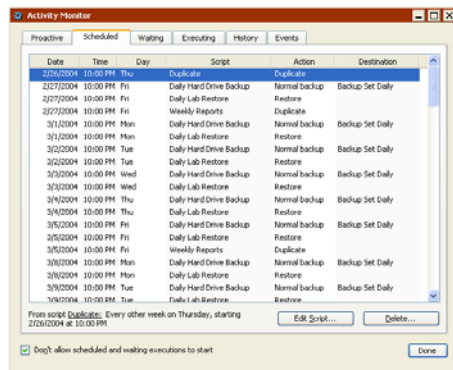
NOTE: Retrospect's Schedule preference (see page 264) defines the time period during which scripts are allowed to execute. Scripts scheduled to execute outside this period will not run.

Retrospect checks the computer's clock and compares it to the next time a script is scheduled to run.

Retrospect is ever-vigilant about scheduled script executions. If a script is scheduled for automatic execution within the look ahead time (normally twelve hours), Retrospect will not automatically quit (or shut down or restart, depending on a preference setting described in

It instead remains open and waits to execute the script.

For more information about the Activity Monitor's Scheduled tab, see "Scheduled Tab" on page 155.

TESTING SCRIPTS

You can check the validity of a script from the script summary window at any time. Retrospect lets you know if the script is missing any required information or if it's ready to run. If the script requires storage media, you can also check to make sure it's ready and available.

To test a script:

1. From the Retrospect navigation bar, click Automate> Manage Scripts.

2. Double-click the script you want to test.

The script summary window displays.

3. Click the Check icon ✓ in the toolbar.

Retrospect displays a dialog reporting on the validity of the script, as well as the next time the script is scheduled to run.
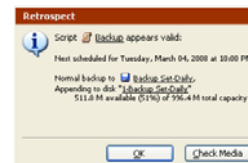
If the script is invalid, Retrospect provides information on what is wrong with the script.

4. If the script is valid, and it requires media, you can click the Check Media button to make sure the backup device is ready with the required media.

5. Click OK to return to the script summary window.

EXECUTING SCRIPTS

Retrospect provides several ways to execute scripts:

• Automatic Script Execution

• Manual Script Execution

For information on interacting with and controlling scripts, see "Controlling Scripts," which starts on page 140.

Automatic Script Execution

"Scheduling Scripts," which starts on page 134, describes how to schedule times for Retrospect to automatically execute a script. Retrospect keeps track of all your scheduled scripts and automatically executes them at the time you specified. The Activity Monitor window (described in "Viewing Scheduled Scripts" on page 262) shows upcoming scheduled events.

Manual Script Execution

To initiate a script manually, you can:

• Execute the script immediately from within Retrospect.

• Make a "run document" file that enables you to run the script at any time, upon your command, from your desktop (or wherever the file is saved).

Use the Manual Script Execution dialog to specify the method you want. There are three ways to access the Manual Script Execution dialog:

• Click the Save and Run button 📝 from the script summary window's toolbar.

• Choose the script from Retrospect's Run menu.

• Click the Run Script button 📝 from Retrospect's main toolbar, then select a script and click OK.
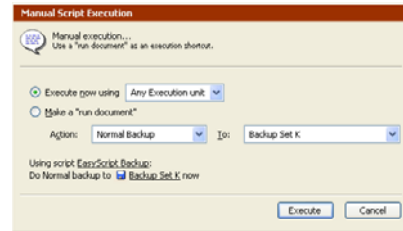
To execute the script immediately:

1. Select the Execute now radio button.

The execution unit list box (if available) lets you override the selection you saved with the script. See "Assigning Execution Units" on page 162 for more information on execution units.

If the script being run is a backup script, use the Action list box to set the backup type. See "Backup Actions" on page 24.

If the backup script has multiple destinations, use the other list box to specify the destination Backup Set.
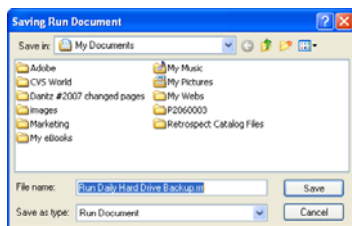
2. Click Execute.

To make a run document:

1. Select the Make a "run document" radio button.

If the script being run is a backup script, use the Action list box to set the backup type. See "Backup Actions" on page 24.

If the backup script has multiple destinations, use the other list box to specify the destination Backup Set.

2. Click Save.

3. Browse to a location to save the run document, enter a file name, then click Save.

WARNING: Do not change the file extension. All run documents must have the extension *.rrr*.

4. Double-click the run document from the desktop or Windows Explorer, to execute the script.

To run several scripts sequentially, select the run documents and choose Open from the File menu. When you open several run documents at once, the scripts associated with them will run in alphabetical order by script name, regardless of the run document file names.

TIP: You can create more than one run document for the same script, each specifying a different backup action and destination Backup Set.

CONTROLLING SCRIPTS

You can control automated operations in much the same way that you control immediate operations. See Chapter 6 • Controlling Operations for more information.

There are a number of preferences that are specific to scripts that must be set correctly. Scripts are designed to run unattended, even after you've quit Retrospect and gone home for the night. Make sure that you have selected the Retrospect's Startup preferences to enable the Retrospect Launcher service and to allow the application to automatically launch to run scripts. See "Startup Preferences" on page 266 for more information.

The Startup preferences also determine what Retrospect does when it has auto-launched and is finished executing the script. By default, Retrospect quits, unless Proactive Backup is running or another script is scheduled to run in the application's look ahead time. See "Schedule Preferences" on page 264 for more information.

If you manually launch a script, you can use the "Stay in Retrospect" list box in Retrospect's toolbar to determine what Retrospect does when it is finished executing. By default, Retrospect does nothing, but if you want to start script and then go home, you can choose to have Retrospect quit when the execution is complete. Unless Proactive Backup is running, or another script is scheduled to run in the application's look ahead time, Retrospect will quit (or shut down) when done. See "Schedule Preferences" on page 264 for more information on specifying the look ahead time.

PROACTIVE BACKUP SCRIPTS

Backup scripts are powerful and versatile, but in backup environments that change regularly, another kind of operation—Proactive Backup—may be better suited to your needs. A regular backup script copies specific volumes in a certain order to a designated Backup Set. If the backup environment changes and volumes or media become unavailable, the backup will not happen until its next scheduled time, if ever. This is why Retrospect offers a Proactive Backup option.

NOTE: Proactive Backup is only available if you have the appropriate license code. Click Configure>Licenses to view your current licenses or purchase new ones.

Proactive Backup Benefits

Retrospect's Proactive Backup technology accommodates changing network and disk

configurations. Whereas a regular backup script follows a rigid schedule for its clearly defined source volumes and destination Backup Sets, a Proactive Backup script is driven by the availability of those resources and their need for backup. Source volumes are backed up in order according to need—that which was backed up least recently is first to be backed up. The volumes are copied to the best available Backup Set media, so Proactive Backup scripts give you greater freedom to use the media of your choice.

Proactive Backup scripts are ideal for environments in which computers and volumes irregularly appear on the network. For example, in an office that has ejectable disks and mobile computers that appear on the network at unpredictable times, Proactive Backup recognizes the new volumes when they become available and backs them up. Client users can even initiate backups of their volumes.

Though Proactive Backup scripts can be used independently, it is often best to use them in concert with regular backup scripts to produce a comprehensive backup strategy.

How Proactive Backup Works

You start with a Proactive Backup script, which is similar to other Retrospect scripts. The backup computer running the script becomes "proactive" during its scheduled time of operation and is idle during its scheduled period of inactivity. You may want to dedicate a computer to Proactive Backup operations during periods of activity and avoid running other programs while Proactive Backup is active.

Proactive Backup makes a queue based on the most recent backups of the source volumes. The least recently backed up volume is moved to the head of the queue and other volumes are arranged in descending order according to the priority of need. Then Proactive Backup examines the local computer and polls the network, looking for the volumes.

NOTE: Polling the network does not adversely affect network performance.

Proactive Backup starts at the top of the volumes queue, determining the availability of each source volume and, if there is a choice, backing up each to its most suitable Backup Set. Retrospect moves the most recently backed up volumes to the bottom of the queue as it goes along. When it is satisfied that all available source volumes are backed up for the current backup interval, Proactive Backup periodically polls clients on the network. Polling involves checking for volumes that have recently appeared, and checking whether any client users have requested backups of their volumes. This whole process ensures a volume in need of backing up gets it.

If allowed by the backup administrator and Proactive Backup, a client user can, at any time, request to be backed up as soon as possible. When Retrospect next polls the client, it will recognize the ASAP request and back up the client.

When the Proactive Backup script's wrap up time is reached, Retrospect continues the current volume backup but will not start any new backups. When the script's stop time is reached, Retrospect halts the backup in progress, if any, and will not start any new backups until the script's next scheduled start time.

NOTE: Proactive Backup uses only the Normal backup action because New Member, Recycle, and New Backup Set backups are inappropriate for use with Proactive Backup scripts.

When to Use Proactive Backup

The following table includes information comparing standard backup scripts to Proactive Backup Scripts

.

Feature	Backup Script	Proactive Backup Script
Destination Backup Sets	Copies to a single Backup Set as specified in the schedule or at execution. Fails if media is unavailable. Media rotation is scripted.	Copies to the most ideal available Backup Set in the destinations list. Automatic media rotation among multiple available Backup Sets.
Source Volumes	Backs up volumes in the order of the source list. If a backup fails, the next backup does not occur until the next time the script runs.	Backs up volumes in the priority order of their most recent backup dates. After each backup, the queue is re-evaluated, including previously unavailable volumes.
Schedule	Starts backup at a specific time and stops when the last source is completed. Optionally ends at a specific time.	Runs between start and stop times. Backups of available volumes occur as necessary.
User Requested Backups	No.	Yes.

See "Network Backup Strategies" on page 225 for descriptions of situations which are suited to Proactive Backup and for instructions on implementing a strategy based on Proactive Backup.

Managing Resources

With abundant resources (large storage capacity, fast network, and powerful backup computer with plenty of time to operate) and relatively few source volumes, Proactive Backup can completely back up all volumes during its window of opportunity. However, with limited resources (small storage capacity, slow network, slow backup computer with little time to operate) and relatively many source volumes, Proactive Backup is not likely to completely back up each volume during its given time period. Fortunately, Retrospect's Proactive Backup effectively manages limited backup resources so that it eventually completes all of its backups.

Trust Proactive Backup to Do Its Job

Whether your setup is resource-constrained or resource-abundant, Proactive Backup always backs up the volumes in order starting with those which need it most. For example, if you need to back up 100 client computers but you can do backups only during an eight hour period each night, chances are Retrospect will be unable to back up all 100 clients the first night before the script's eight hours are up. Leftover volumes will be backed up the next night, and so on, until all 100 volumes are backed up. After the initial backups, Proactive Backup will move more quickly through the queue as it performs subsequent Progressive Backups.

As the backup administrator, you do not have to separate the clients into different groups for different days based on your estimation of backup times. Proactive Backup distributes the load over the scheduled time period.

The main thing to remember about Proactive Backup is that all of the source volumes eventually are backed up with no additional effort on your part. In the worst case, the period of time between backups of a given volume will be too long for comfort and you must allot more resources.

If you want your volumes to be backed up more often than they are, you must allocate more resources to the Proactive Backup script. Increase the script's operating time, use selectors to limit the files to back up, use a faster backup computer, or speed up your network. Setting up a second backup computer with Proactive Back-

up handling half of your clients effectively divides the load in half for each backup computer.

Monitoring Progress

Periodically view the Backup Report (see page 229) to see which volumes were backed up by Proactive Backup and their intervals between backups. Of particular interest is the "Elapsed Days" column which shows how many days have passed since each volume's previous backup.

NOTE: The interval between backups will tend to be smaller when Retrospect is performing Progressive Backups after the first backup of each volume. Progressive Backups require far less time for most volumes and thus can occur more often.

Deleting a backup event from the Backup Report causes Retrospect to not consider that backup occurrence when it evaluates the priority of volumes to be queued for backup. Consequently, that volume is given a backup priority higher than its previous priority.

Interaction with Other Scripts

You can use multiple Proactive Backup scripts operating simultaneously to manage limited backup resources. You can also use multiple scripts with different schedules to give some volumes a higher backup priority.

For example, one script could run eighteen hours a day, backing up volumes from the sales department. Another script could run six hours a day, backing up volumes from the accounting department. The sales department would be more likely to get completely backed up, whereas the accounting department script may not complete all its volumes in a single six hour period. Still, these volumes would eventually get backed up because volumes in greatest need of backup are backed up before volumes which have more recent backups.

As another example, consider volumes that are available intermittently, such as removable disks and notebook computers. Another script could back them up twenty-four hours a day, because they are available at random times during the day.

For further discussion of Proactive Backup strategies, see "Backup Strategies," which starts on page 224.

Other, non-Proactive Backup scripts scheduled for execution during the active operating time of Proactive Backup scripts can run without conflict.

Proactive Backup Tips and Techniques

To get the most out of Proactive Backup, you should follow a few simple guidelines.

Choose the Right Proactive Backup Computer

The computer you use for Proactive Backup is important. Proactive Backup scripts work best on a dedicated backup computer that is not running other file serving or sharing software. Proactive Backup runs best on a backup computer with a powerful processor.

Proactive Backup does not quit or shut down the backup computer when it is finished; rather, it waits idle until the next scheduled start time.

Use Containers as Sources

Use containers (see page 281) to specify sources in your Proactive Backup scripts, not individual volumes, especially when you back up clients. When you use containers, any new volumes added to a client are automatically included in backups.

Rotate Among Backup Sets

Create multiple Backup Sets and use them all as destinations in your Proactive Backup script. Rotate through the sets by inserting different

media in the backup device each day. Proactive Backup uses whatever media you inserted.

Introduce New Media

Periodically do New Backup Set backups to introduce new media. Store old media off-site after each New Backup Set backup. Between New Backup Set backups, periodically do Recycle backups to prevent Catalogs from becoming cumbersome and to ensure fast restore operations.

When you want to rotate or introduce new media, do Recycle or New Backup Set backups by executing regular backup scripts using the same Backup Sets used by your Proactive Backup scripts. You can schedule these, execute them from Retrospect's Run menu, or save them as run documents and execute them.

To manually set a Backup Set for a Recycle or New Backup Set backup, configure the Backup Set and set the media action. (See "The Options tab" on page 256).

Monitor Media Availability

Because Proactive Backup does not initially put up media request windows, you have to monitor media from the Activity Monitor. Click Activity Monitor>Proactive to check on your Proactive Backup Scripts.
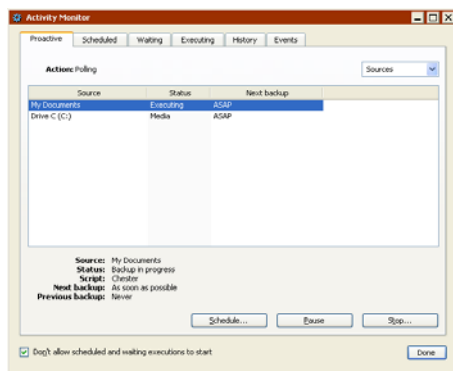
When Retrospect needs media it displays "media" in the status column of the Sources or

Backup Sets view. Choose Backup Sets from the list box to see which destination Backup Sets have media available and which do not. Insert media as needed.

If a Backup Set needs a new or erased medium and you have to erase one, stop Proactive Backup, erase the medium from Configure>Devices, then start Proactive Backup again.

Use Other Scripts to Complement Proactive Backup

Retrospect can have multiple Proactive Backup scripts running concurrently, and it will manage the sources and destinations.

Other, non-Proactive Backup scripts can execute while Proactive Backup is running. You can schedule them or run them at will using run documents. Other scripts can complement Proactive Backup scripts by starting Recycle and New Backup Set backups, and by forcibly backing up volumes that do not get backed up by Proactive Backup.

Use Tape Libraries

An automatic tape loading device with Proactive Backup is a powerful combination. All tapes in the library's magazine are available for backup as Backup Set destinations. Proactive Backup rotates between Backup Sets with no additional effort from you. It uses blank or erased tapes when a backup spans over two tapes, or when you set up a New Backup Set backup with Retrospect's media action options.

Allow Early Backups

By default, Proactive Backup scripts allow early backups. These occur when Proactive Backup is polling through the list of possible sources and finds a client that has requested to be backed up as soon as possible. When a client user selects this option in his or her Retrospect Client control panel, the client software does *not* send a message to Retrospect on the backup computer. Rather, Retrospect contacts clients as

Proactive Backup polls, which it does when it is not actually performing backups during its scheduled active time.

If many clients are due for backup, a client with a current backup may wait a long time before Proactive Backup gets to it. Regardless of the client user's desire for backup ASAP, Retrospect backs up other clients that do not have current backups. Retrospect always polls starting with clients who need backups the most.

For more information, see "Proactive Backup Interval Options" on page 236.

Manage User Deferments

When a client user repeatedly defers his or her backups (as indicated in the Operations Log), you should make future backups occur at a time that is more convenient for the user, such as when he or she is not using the computer. Or, create a script with the countdown time option at zero to prevent the user from deferring execution.

Set Priority by Volumes

If certain critical volumes are not getting backed up as often as you would like, consider using multiple scripts with different schedules to give some volumes higher backup priority than others. Schedule the higher-priority volumes script to run for a longer duration than the lower-priority volumes script. With more time allotted to the higher-priority volumes, they are more likely to get completely backed up.

Set Priority by Files

If you find Proactive Backup is not completely backing up all its sources, another way to set the backup priority is by files rather than volumes, though you can also do both. Use multiple scripts with different selectors to give some files or folders higher backup priority than others. For example, a higher-priority selector would include documents modified in the last seven days, and a lower-priority selector would include all files. Schedule the higher-priority

script to run for a longer duration than the lower-priority script.

Creating Proactive Backup Scripts

This section takes you through the steps of creating a Proactive Backup script: The process is very similar to creating a regular backup script, although Proactive Backup scripts are scheduled differently.

To create a Proactive Backup script:

1. From the navigation bar, click Automate, then click the Proactive Backup button.

The Proactive Backup window displays.
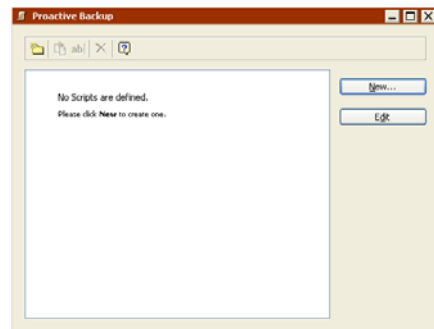
2. Click the New button to create a new script, then enter a name and click New.

The script appears in its own window.
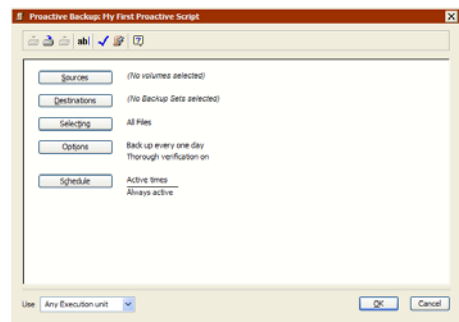
This script window is very similar to a regular backup script summary window, with information for the source volumes, destination Backup Sets, file selection criteria, options, and schedule information.

3. To change information, click the appropriate button.

Sources lets you add or remove source volumes.

Destinations lets you choose one or more destination Backup Sets.

Selecting lets you choose a selector—a kind of filter for selecting files and folders to be backed up.

Options displays the options window in which you can toggle verification and data compression.

Schedule lets you set the script to run all the time or only on specific days at specific times. The execution unit list box (if available) lets you choose a specific execution unit (or use any execution unit) for this Proactive Backup script..

Setting the Proactive Backup Sources

The first step in defining a Proactive Backup script is setting the sources.

1. Click the Sources button.

The Source Selection window displays.
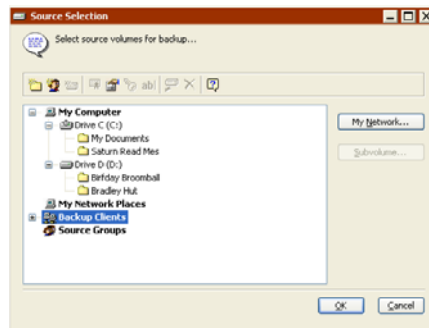
2. Select a source volume (or volumes), then click OK.

NOTE: Proactive Backup scripts are especially well-suited for backing up laptop client volumes, or other volumes that appear irregularly on the network.
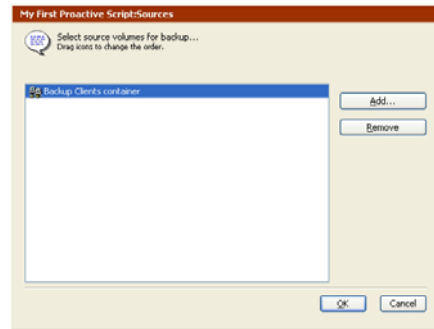
3. Click Add to select additional sources, or select a source and click Remove to remove it from the list. When the list of sources is complete, click OK.

NOTE: If your script includes multiple sources, they are backed up according to need and availability.

Setting the Proactive Backup Destination

After specifying the source(s) to back up, you must specify the destination Backup Set(s) for the data.

1. Click the Destinations button.

If there are no Backup Sets defined, the Backup Set Creation Wizard launches.

Create a new Backup Set, as described in "Creating Backup Sets" on page 252. The new Backup Set appears in the Backup Set Selection window.

If there are Backup Sets defined, the Backup Set Selection window displays.

You can click More or Create New to access additional Backup Sets or create new ones.

2. Select one or more Backup Sets, then click OK.

3. Click Add to select additional destinations, or select a Backup Set and click Remove to remove it from the list. When the list of destinations is complete, click OK.

Selecting Files for Proactive Backup

By default, Retrospect selects all files on the source(s). You can choose a different pre-defined selector or create a custom selector to select a subset of all files.

1. Click the Selecting button.

2. Click a selector, then click OK.

You can also click More Choices to use Retrospect's file selection criteria to create a custom selector. Selectors are explained in

detail in "Using Selectors," which starts on page 291.

NOTE: Selectors are used to determine which files are *considered* for backup, not which files actually get copied. For example, if you choose All Files, Retrospect compares all the source files with the files already in the destination Backup Set, then copies *only* those files that are new or changed.

Setting Proactive Backup Options

Click the Options button to display the options window in which you can specify how often to back up source volumes and whether or not to allow early backup. Click More Choices to see all of the available options categories and notice that many categories parallel those of regular backup scripts. Categories specific to Proactive Backup scripts are Interval, Countdown, and Polling. These options are explained in detail in "Execution Options," which starts on page 236.

Setting the Execution Unit

If your edition of Retrospect is capable of running multiple simultaneous executions, you can specify which execution unit to use for this operation (or choose "Any Execution unit"). Make your selection in the summary window's list box. See "Assigning Execution Units" on page 162 for more information.

Scheduling Proactive Backup Scripts

A Proactive Backup script's schedule is one of the major differences between it and a regular backup script. From the script summary window, click the Schedule button.
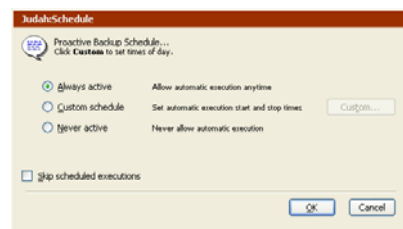
Select a schedule:

- **Always active** makes Retrospect run the script twenty-four hours a day, seven days a week.
- **Custom schedule** brings up another window in which you can customize the script schedule. See "Customizing the Schedule".
- **Never active** prevents Retrospect from running the script.

The **Skip scheduled executions** checkbox prevents Proactive Backup from running until the time you specify.

Customizing the Schedule

By default, Proactive Backup scripts are active 24 hours a day, 7 days a week. If you want to specify different hours or days for a script to be active, you can create a custom schedule.

When you select Custom schedule and click Custom, Retrospect displays the custom schedule window. Though similar to the Schedule Preferences window, it is specific to this Proactive Backup script rather than global to all Retrospect executions.
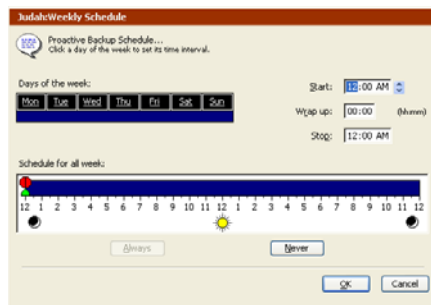
If the schedule was previously Always Active, all twenty-four hours of each of the seven days of the week are selected, as above.

To select a day of the week, click on it. Click and drag to select contiguous days of the week. Use the Shift or Control key and click or drag to select days without de-selecting the previous selection.

To change a time, click on it and type or use the control.

Start is the time at which the script begins.

Wrap up is the period of time (in hours and minutes) before the stop time, during which Retrospect should complete the current backup but not begin new backups.

Stop is the time at which Retrospect absolutely must halt this script's backups (until the next start time).

TIP: You can also set times by dragging the icons on the hourly schedule bar, but you should first experiment by typing the times to see how these controls work.

When a time is changed, the hourly schedule bar changes accordingly to graphically represent the start, wrap up, and stop times of the script.
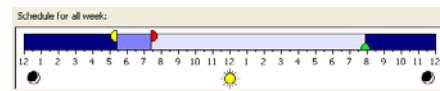
Each selected day has a scaled-down hourly schedule bar, though it does not have controls.

You can revert a customized schedule with the Always and Never buttons.

Controlling Proactive Backup

There are a number of ways to control Proactive Backup and Proactive Backup scripts, both from the Retrospect application and from Retrospect clients.

You can control Proactive Backup from Retrospect's Run Menu and the Activity Monitor's

Proactive tab. You can control Proactive Back-up scripts from the Retrospect Client Control Panel and the Activity Monitor's Proactive tab

NOTE: Proactive Backup is not affected by the selection in the "Stay in Retrospect" list box in Retrospect's toolbar, or by Retrospect's unattended Startup preference. For example, Retrospect will not quit when a Proactive Backup script is done.

Run Menu

From the Run menu, you can start/stop and en-able/disable Proactive Backup. When you save a Proactive Backup script, Proactive Backup is enabled (unless the script schedule is "never ac-tive") after the backup computer is idle for ten minutes. Retrospect starts Proactive Backup when a script's scheduled start time arrives. If Retrospect is not open at the start time, it will launch automatically.

You can control Proactive Backup manually by choosing commands from the Run menu:

• Choose Start Proactive Backup to manually enable Proactive Backup. Proactive Backup scripts will then run at their scheduled times of execution. When Proactive Backup is started, you can choose Stop Proactive Backup from the run menu to stop it.

TIP: You can also start/stop Proactive Backup using the Start and Stop buttons on the Activity Monitor's Proactive tab.

When Proactive Backup is stopped, no Proac-tive Backup scripts will run for 10 minutes, or until you start Proactive Backup again.

NOTE: If you exit Retrospect, then relaunch it (or it is auto launched) Proactive Backup will start automatically (after a short delay), unless it is disabled.

• Choose Disable Proactive Backup from the Run menu to prevent any scheduled Proactive Backup scripts from executing.

When Proactive Backup is disabled, no Proac-tive Backup scripts will run until you choose Start Proactive Backup or Enable Proactive Backup.

Activity Monitor

The Proactive tab in the Activity Monitor pro-vides information about Proactive Backup and Proactive Backup scripts.
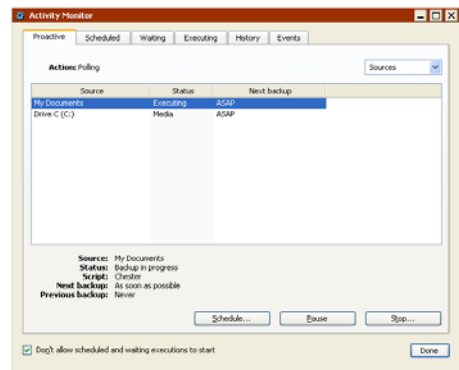
From the Proactive tab, you can pause Proactive Backup scripts, start/stop Proactive Backup, override schedules, and view status. See "Pro-active Tab" on page 153 for more information.

Client Control Panel

You can use the client control panel to request Proactive Backup as soon as possible, or at a specific time. You can also defer a backup that is about to start until a later time.

See "Controlling Proactive Backups" on page 186 for more information.

CONTROLLING OPERATIONS

- **CONTROLLING OPERATIONS OVERVIEW**

- **STOP BUTTON**

- **ACTIVITY MONITOR**

- **MEDIA REQUEST WINDOW**

- **MULTIPLE CONCURRENT EXECUTIONS**

You previously learned how to set up and initiate immediate and automated backup, duplicate, archive, restore, and transfer operations. This section describes how to monitor and control scheduled and executing operations using the Activity Monitor. It also describes how to take advantage of Retrospect's ability to run multiple concurrent executions.

CONTROLLING OPERATIONS OVERVIEW

Retrospect's Activity Monitor allows you to control operations that are executing, as well as scheduled and waiting operations. In addition, the Activity Monitor provides information about operations that have finished executing. To learn more about the Activity Monitor, see "Activity Monitor".

If the media required to complete an operation is not available, Retrospect displays the media request window (except for Proactive Backup scripts). For more information about this window, see "Media Request Window" on page 158.

Retrospect allows you to perform multiple simultaneous executions, provided that the backup computer and backup devices can support this feature. For more information about multiple executions, see "Multiple Concurrent Executions" on page 161.

If you specified password protection for Retrospect using its security preference you can choose Lock Application from the File menu to prevent other users from stopping operations without entering the password. See "Security Preferences" on page 265 for more information.

STOP BUTTON

The Retrospect toolbar includes a stop button that makes it easy to stop all currently executing operations.

If Retrospect is set up with numerous scripts, including Proactive Backup scripts, that run at all times of the day and night, it can sometimes be difficult to manage your scripts and Backup Sets, since Retrospect starts executing the scripts soon after it is launched.

When Retrospect launches and a script is about to run, a countdown dialog displays.
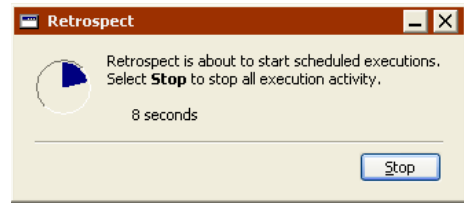
Click Stop, then confirm your selection to temporarily stop all execution activity. If you are unable click Stop before the countdown expires, you can click the Stop all execution activity button in the Retrospect toolbar to achieve the same effect.

Proactive Backup is stopped and scripts are not allowed to start until you click the button in the Retrospect toolbar again. When you click the button again, Proactive Backup starts and Retrospect allows scheduled and waiting scripts to execute.

Clicking Stop also turns off and disables the Automatically launch Retrospect preference until the button is clicked again. See "Startup Preferences" on page 266 for more information.

NOTE: Once you click the Stop button it remains selected even if you exit and relaunch Retrospect. When all execution activity is stopped, the Retrospect icon in the system tray of your Windows taskbar will flash until you click the Stop all execution activity button in the Retrospect toolbar.

ACTIVITY MONITOR

The Activity Monitor provides an interface for viewing and interacting with immediate and scripted operations, before, during, and after they execute. The Activity Monitor automatically displays (on the Executing tab) when an operation is executing. To open it manually, click the Activity Monitor button on the Retrospect toolbar.

The Activity Monitor contains the following tabs:

- Proactive Tab
- Scheduled Tab
- Waiting Tab
- Executing Tab
- History Tab
- Events Tab

Each tab provides a unique set of commands and information about Retrospect activities. One item that appears on all the tabs is the "Don't allow scheduled and waiting executions to start" checkbox. Select this checkbox to prevent any Proactive, scheduled, or waiting execution from starting until the checkbox is deselected.

Proactive Tab

Click Activity Monitor>Proactive from Retrospect's navigation bar to monitor Proactive Backup scripts.
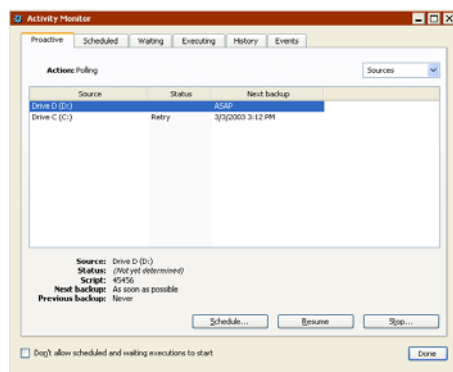
You can start and stop all Proactive Backups, pause and resume specific scripts, and modify the script schedules.

For more information on controlling Proactive Backup and Proactive Backup scripts, see "Controlling Proactive Backup" on page 148.

Once a Proactive Backup script starts, you can monitor the operation's progress in the Executing tab. However, unlike other types of operations, if the required media or execution unit for a Proactive Backup script is not available, the script will not move to the waiting tab or display a media request dialog. Proactive Backup waits until all the required resources are available before beginning the operation.

If the required media is not available the Status column (visible when Sources or Backup Sets is selected in the list box) in the Proactive tab will say "Media". The script will execute automatically when the required media becomes available.

If the required execution unit is not available, the Proactive Backup script will wait until it is.

For more information on execution units, see "General Preferences" on page 264,

Proactive Backup Status

There are three ways to view Proactive Backup script information. Choose one of the following options from the list box:

- **Sources** shows the source volumes used by all running scripts, and indicates the status of each source and the time of the next backup. From the Sources view, you set a specific schedule for backing up any of the script's sources.
- **Backup Sets** shows the Backup Sets used by all running scripts and indicates the status of the operation.
- **Scripts** lists all Proactive Backup scripts by name and indicates their status. From the Scripts view, you can deactivate a script.

Retrospect lists the status of each item under the status heading.

Blank means Proactive Backup has yet to connect with the item.

Active means the script is functioning.

ASAP means the source will be backed up as soon as possible. This may be either because the client user initiated the backup or the client's most recent backup is older than the script's backup interval.

Backed up means the source volume has been backed up within the specified interval.

Busy means that Proactive Backup is waiting for a resource that is currently in use.

Deferred means the client user has intercepted and postponed the backup. Such user deferments are entered in the Operations Log.

Device means that Proactive Backup cannot find the tape drive to which the required Backup Set is bound. See "The Binding tab" on page 259 for more information.

Inactive means the script was deactivated or its schedule does not currently permit it to run.

Media means Proactive Backup cannot find the proper media for the item's Backup Set.

Password means that a Backup Set required by Proactive Backup is password-protected and requires the password for any access. To make the Backup Set accessible, go to Configure>Backup Sets, select the protected Backup Set, and click Properties. Once you enter the password, the Backup Set will be accessible until you re-launch Retrospect.

Ready means a source is currently being backed up or is about to be. It also means a Backup Set is ready as a backup destination.

Retry means Proactive Backup failed to back up the source and will try again.

Scheduled means the source has never been backed up, but the administrator has scheduled a pending backup.

Source means Proactive Backup cannot find the source volume.

Wrap up means a Proactive Backup script is in its wrap up period.

Click on a source, Backup Set, or script to see more status information in the lower part of the Activity Monitor window.

Proactive Backup Commands

The Proactive tab includes the following commands:

- Click the **Schedule** button to override a Proactive Backup script's execution schedule. If Sources is selected in the list box, enter a date and time in the dialog box, then click OK. If Scripts is selected in the list box, select a radio button option for when the script should be active, then click OK.

- Click the **Pause** button to pause *all* pending Proactive Backup script executions.

- Click the **Continue** button to continue *all* pending Proactive Backup script executions.

- Click the **Start** button to start Proactive Backup. If you have created any Proactive Backup scripts, and Proactive Backup is not disabled, it will start automatically after 10 minutes.

- Click the **Stop** button to stop Proactive Backup from running. When you click Stop, no Proactive Backup scripts will execute until you click Start. If you do not disable Proactive Backup, it will automatically start up again after 10 minutes. When you stop Proactive Backup, any schedule overrides you specified while Proactive Backup was running will be lost.

- Choose an item from the **Sources** list box to change the view. Choose Sources to view Proactive Backup scripts based on their source; choose Backup Sets to view Proactive Backup scripts based on their

destination; or choose Scripts to view to view Proactive Backup scripts by script name.

- Select the "Don't allow scheduled and waiting executions to start" checkbox to prevent any Proactive, scheduled, or waiting execution from starting until the checkbox is deselected.

Deactivating a Proactive Backup Script

Retrospect allows you to temporarily deactivate a Proactive Backup script so its sources are not included in Proactive Backup's routine operations.

NOTE: When Proactive Backup is stopped and later started, the script will be active.

To prevent a specific Proactive Backup script from executing, first click the Scripts tab. Then select the script from the list and click Schedule from the toolbar and in the dialog that follows select Never active and click OK.

Reactivating a Script: To allow a deactivated Proactive Backup script to execute and include its sources in Proactive Backup's routine operations, follow the same steps as deactivating but select Always active.

Scheduling a Backup of a Source

Retrospect allows you to schedule a backup of a source from a running Proactive Backup script. This lets you set a definite time for Proactive Backup to back up the source, rather than wait for Proactive Backup to back it up at its convenience. This is useful, for example, when the backup administrator knows a salesperson will be leaving the office with her notebook computer. The administrator can schedule that client for backup immediately.

To schedule a backup of a source, first click the Sources tab in the Proactive Backup status window. Then select the source from the list and click Schedule from the toolbar (or double-click on the source).
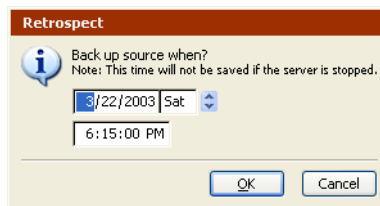
Use the controls to set the date and time to back up the source, then click OK. Retrospect changes the priority of the source in the Proactive Backup queue according to your scheduled time.

NOTE: A backup scheduled this way is not remembered by Retrospect when Proactive Backup is stopped.

Scheduled Tab

Click Activity Monitor>Scheduled from Retrospect's navigation bar to preview upcoming scripts (excluding Proactive Backup scripts).
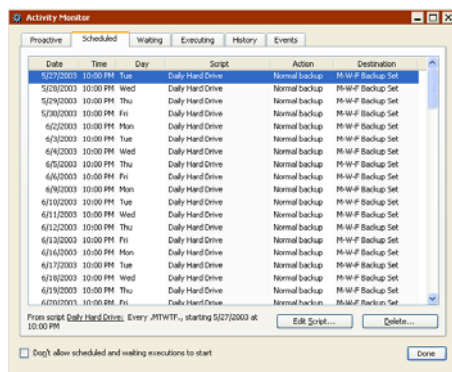
You can edit and delete specific scripts from this window, and also prevent all scheduled executions from starting.

The Scheduled tab includes the following commands:

- Click the **Edit Script** button to display the script summary window. From this window, you can modify the script sources, destinations, selected files, options, and

schedule. Make your changes, then click OK.

- Click the **Delete** button to delete the script execution for the selected date and time, as well as all other executions of the script scheduled prior to the selected date and time. Retrospect displays a dialog asking you to confirm the request.

- Select the **"Don't allow scheduled and waiting executions to start"** checkbox to prevent any Proactive, scheduled, or waiting execution from starting until the checkbox is deselected.

Once a script's scheduled execution time arrives, it moves from the Scheduled tab to the Executing tab, or, if the required resources are not available, to the Waiting tab.

Waiting Tab

Click Activity Monitor>Waiting from Retrospect's navigation bar to view operations that are waiting for resources (Backup Sets, sources, execution units.).
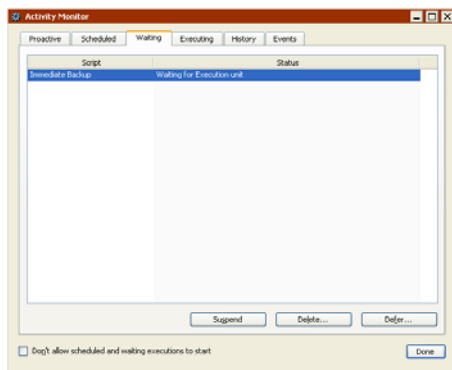
For example, if an operation requires a specific execution unit that is already in use, or if all available execution units are currently in use, the operation will get put into the waiting queue. For more information about execution units and multiple simultaneous executions, see "Multiple Concurrent Executions" on page 161.

The Waiting tab includes the following commands:

- Click the **Suspend** button to pause the selected operation. Suspended operations will not execute until they are resumed (even if the required resources become available).

- Click the **Resume** button to resume a selected suspended operation. When the resources required to run the operation become available, it will execute.

- Click the **Delete** button, then click OK to delete the selected operation.

- Click the **Defer** button to defer execution until a specified a date and time. At that date and time (provided you have not quit Retrospect in the meantime) the operation will try to execute. If the required resources are available, it will execute. Otherwise, it will get placed in the waiting queue.

- Select the "Don't allow scheduled and waiting executions to start" checkbox to prevent any Proactive, scheduled, or waiting execution from starting until the checkbox is deselected.

Once an operation starts executing, you can monitor its progress in the Executing tab.

Executing Tab

Click Activity Monitor>Executing from Retrospect's navigation bar to view executing operations.
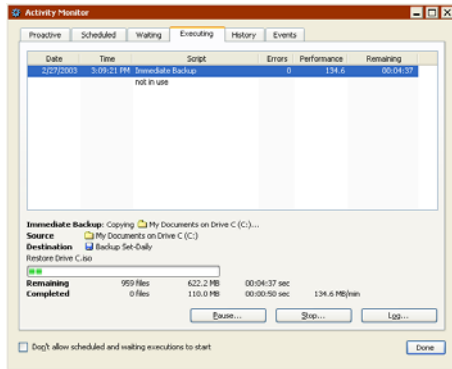
When an operation begins executing, the Activity Monitor's Executing tab displays automatically.

You can monitor the performance of currently executing operations, temporarily pause, or permanently stop an operation, and view the log associated with an operation. If the operation requires media that is not available or accessible, the Media Request window displays during execution.

NOTE: What Retrospect does after the operation is complete depends on whether it's an immediate operation or a scripted operation and the preferences you have specified. See "Startup Preferences" on page 266 and "Schedule Preferences" on page 264 for more information.

While an operation is executing, it includes the following commands:

- Click the **Pause** button, then click Yes to temporarily suspend the selected operation. If you want to pause *all* executions and/or not allow scheduled and waiting executions to start, select the appropriate checkbox(es), then click Yes.

- Click the **Continue** button, then click Yes to resume the selected operation. If you want to continue *all* executions and/or allow scheduled and waiting executions to start,

select the appropriate checkbox(es), then click Yes.

- Click the **Stop** button, then click Yes to halt the selected operation, bringing it to a premature end. If you want to stop *all* executions and/or not allow scheduled and waiting executions to start, select the appropriate checkbox(es), then click Yes.

- The **Log** button displays Operations Log information for the selected operation.

If the media required for the selected operation is not available, Retrospect displays a media request dialog. See "Media Request Window" on page 158 for more information.

Once an operation is complete, it is removed from the Executing tab. Click the History tab to view details about the operation.

History Tab

Click Activity Monitor>History from Retrospect's navigation bar to view operations that are finished executing (successfully or unsuccessfully).
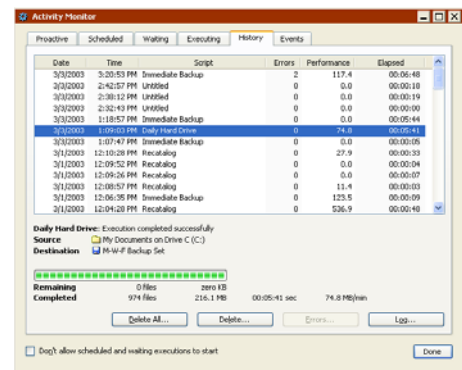
The History tab includes information about the date, time, and performance of the most recent operations and has the following commands:

- Click the **Delete All** button, then click OK to clear history information for all listed items. If you don't delete the operations history, Retrospect automatically removes the oldest

operations to display information about more recent operations. Use the Execution history limit to control the maximum number of operations listed in the History tab. See "General Preferences" on page 264 for more information.

- Click the **Delete** button, then click OK to clear history information for the selected operation.
- Click **Errors** to display a browser listing the file(s) that caused the error. The Error button is only enabled if there is a file-related error. Other errors are explained in the Log.
- Click the **Log** button to display the Operations Log information for the selected operation.

Events Tab

Click Activity Monitor>Events from Retrospect's navigation bar to see special messages from Retrospect concerning past and current operations.
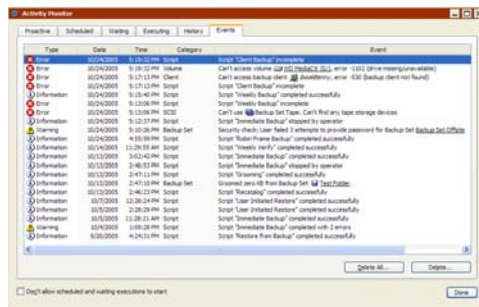
For each event, Retrospect displays information about the event type, the date and time of the event, the event category, and a brief description of the event. You should periodically review the Events tab as part of your regular monitoring of the Retrospect backup computer.

Event types include Information, Warning, and Error. Information events are displayed for operations that complete successfully or are stopped before completion. Warning events can

be more serious. For example, if a backup completes with errors, Retrospect displays a Warning event. Finally, Error events are the most serious. Retrospect displays an Error event when it cannot complete an operation, for example, if a script fails or a volume or device is not accessible.

Each event displayed by Retrospect falls into one of the following categories: Volume, Client, Device, SCSI, Backup Set, Engine, or Script.

You can delete a selected event or delete all events using the following commands:

- Click the **Delete All** button, then click OK to delete all events. If you don't ever delete events, Retrospect automatically removes the oldest events to display information about more recent events. Use the Execution event limit to control the maximum number of events listed in the Events tab. See "General Preferences" on page 264 for more information.
- Click the **Delete** button, then click OK to delete the selected event.

TIP: All Retrospect events are also logged in the Windows Event Viewer's Application log (not available with Windows 98/Me). See your Windows documentation for information on accessing the Event Viewer. If you select Retrospect's "Enable notification for external applications" preference, certain applications, such as EMC Legato Networker Management Console, can also display Retrospect events. See "Reporting Preferences" on page 272 for more information.

MEDIA REQUEST WINDOW

When an operation moves into the Activity Monitor's Executing tab and the required media is not available, Retrospect prompts you to insert media with the correct name or blank or

erased media, by displaying a media request window.

You can avoid this prompt if you insert the correct medium before the operation executes. So it does not overwrite valuable data, Retrospect is very particular about tapes, discs, and removable disks—they must be blank or erased, or their names must exactly match the requested names in order for Retrospect to proceed without prompting you. When performing new or Recycle backups, consider erasing removable media or adding hard disks beforehand to be sure Retrospect will proceed automatically without a media request.

The media request window looks different depending on whether your destination is a tape/CD/DVD Backup Set or a disk Backup Set.

Tape/CD/DVD Media Request

When backing up to tapes or CD/DVDs, the media request window looks a lot like the Storage Devices window.
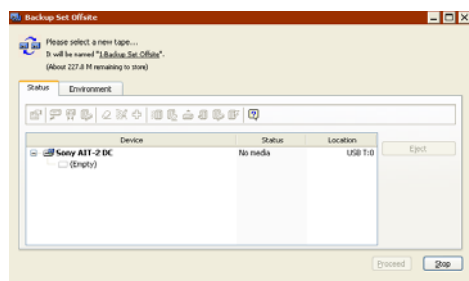
Click Stop to halt the current operation. If Retrospect is looking for new media, insert blank/erased media and click Proceed to continue the current operation. If Retrospect is looking for a specific named member of a Backup Set insert it and click Proceed. If the named member is unavailable click Choices (see "Media Unavailable" for more information).

The window has a toolbar with the same commands available from the Storage Devices window. See:

- "Toolbar Commands for Discs" on page 35
- "Toolbar Commands for Tape Drives" on page 44
- "Toolbar Commands for Tape Libraries" on page 47

The most useful commands during a media request are:

Eject: unloads the selected medium from its drive so you can insert the correctly named medium or a blank/erased tape/CD/DVD.

Erase: erases the contents of the selected tape or CD/DVD and then uses the erased medium for the current operation.

Media Unavailable

If the requested media is unavailable, click the Choices button. The media choices dialog displays. Choose one of the following options:

Missing: tells Retrospect to designate the requested member as permanently unavailable from the Backup Set. Retrospect will ask for a new member and, if possible, copy the missing data to it during the next backup or archive.

Select Missing only when you have permanently lost or damaged the requested member. It is not appropriate for other situations.

Skip: tells Retrospect to skip the requested member and ask for a new member. Data on the requested member remains intact. Effectively, you are saying, "Stop copying to this member and start copying to a new one." This is useful when a member is nearly full and you think it may not make it through a complete unattended backup before Retrospect fills it and asks for a new medium.

WARNING: Do not select Skip when you have lost or damaged the requested medium, or you may lose your data. Select Missing instead.

Disk Media Request

When backing up to disk, the media request window looks a lot like adding a disk to a new disk Backup Set. The window displays when the disk is full or unavailable to Retrospect.
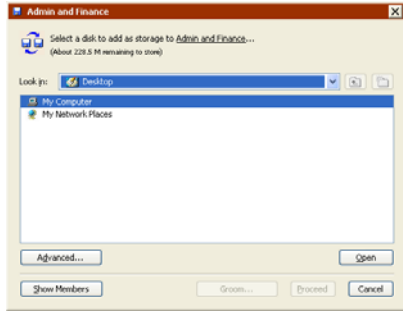
Click Cancel to halt the current operation.

Click Show Members to show all members of the Backup Set and view details about each with the Properties button. If any of the existing members has more disk space available, you can add it to the Backup Set in the Properties window. If you are able to add enough space, Retrospect continues the current operation.

Browse to and select a disk with available space and click Proceed to add it as a member of the Backup Set. Retrospect displays a window that summarizes information about the disk you are adding and lets you specify how much storage space to dedicate to the Backup Set.
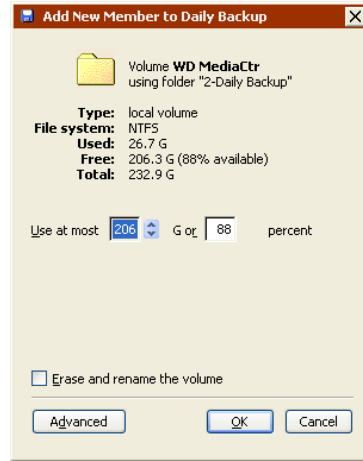
Click the Advanced button, to specify additional options.

- A location for the backup data folder. If you don't specify a location, the folder is automatically saved on the root level of the disk.
- A password for a network volume so Retrospect can automatically log in during unattended backups.

NOTE: With non-system local volumes, you can also have Retrospect erase and rename the disk.

Click OK to add the disk and continue the current operation.

For disk Backup Sets with grooming enabled, Retrospect only displays the media request window after it has already groomed the Backup Set and determined that it still needs more disk space to complete the current operation. If the Backup Set is grooming to the Retrospect defined policy, you must add another disk (or increase the space available to the current disk) to continue the current operation.

If the grooming policy specifies the number of backups to keep, you can click Groom to decrease this number and delete older Snapshots

and their associated files to reclaim disk space on the current Backup Set member. This frees up room for the current operation, but the groomed data cannot be recovered.
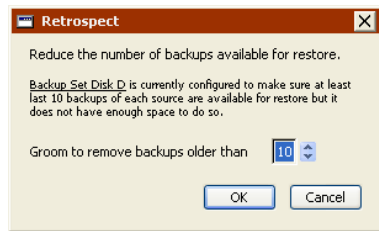
Click Groom, then enter a new, reduced number of backups to keep and click OK. Retrospect grooms the Backup Set and, if it now has enough available disk space, continues the current operation.

MULTIPLE CONCURRENT EXECUTIONS

Retrospect allows you to: change configuration settings while and operation is executing; execute independent operations in parallel; handle resource conflicts (including serializing conflicting executions); have the Proactive Backup system kick off multiple executions; and use multiple drives in a tape library simultaneously.

Retrospect has both core multiple execution capabilities and additional capabilities (support for simultaneous use of multiple tape drives) that are enabled through the Advanced Tape Support add-on.

NOTE: Retrospect Professional does not support multiple concurrent executions.

Multiple Executions

Retrospect comes pre-configured for multiple execution units, the exact number of which is based on the backup computer's total amount of memory.

NOTE: The software allows up to 8 concurrent executions, provided the computer has enough memory and backup devices to support such a configuration.

When you're using multiple execution units, you can run multiple operations at the same time. If you start more operations than there are available execution units, the additional operations are placed in a "Waiting" queue until an execution unit becomes available. See "Waiting Tab" on page 156.

NOTE: Proactive Backup scripts and User Initiated Restore operations do not go into the waiting queue. They only launch when an execution unit (and other required resources) is available.

Generally, in order to execute operations concurrently, the operations must each have a unique source and a unique destination. Disk Backup Sets are unique in that the same Backup Set can be used as the destination in one operation while, at the same time, as the source for one or more additional operations. This feature is discussed in "Disk Backup Sets and Multiple Executions".

Subvolumes and mailboxes are *not* considered unique from the volume or Exchange Mailbox container on which they are stored. Therefore, you cannot back up from or restore to a volume and any of its subvolumes (or an Exchange Mailbox container and any of its mailboxes) concurrently. Retrospect will run these executions consecutively.

If you have multiple disk Backup Sets stored on the same disk, Tqzkq recommends that you not use those Backup Sets in concurrent operations.

Disk Backup Sets and Multiple Executions

Retrospect server-class editions are unique in that they support a single write operation and

multiple read operations simultaneously using the same disk Backup Set.

Write operations include:

- Backing up to the Backup Set
- Transferring to the Backup Set
- Archiving to the Backup Set

Read operations include:

- Restoring from the Backup Set
- Transferring from the Backup Set
- Preparing for disaster recovery
- Viewing the Backup Set Properties
- Browsing a Backup Set's Snapshots or Sessions

As long as you have enough execution units available, you can perform one write operation at the same time as one or more read operations. You can also perform multiple read operations at the same time.

For example, you can back up to a Backup Set, while simultaneously restoring a Retrospect Client from the same Backup Set. You can also:

- Perform multiple restores (including User Initiated Restores) from the same Backup Set
- Transfer Snapshots from a Backup Set while backing up to that Backup Set

The only limitation, other than execution units, is that none of the concurrent operations can require same volume/database/mailbox or the same non-disk Backup Set.

NOTE: Certain operations require exclusive access to the Backup Set (e.g. updating a Catalog File, grooming, recycling, verifying media). When one of these operations is using a disk Backup Set, no other operations can use that Backup Set at the same time.

To take full advantage of these disk Backup Set capabilities, make sure your scripts specify that Retrospect use "Any Execution Unit". See "Assigning Execution Units" on page 162 for more information.

Other than specifying "Any Execution Unit" in your scripts, there is nothing you have to do to use this feature. Scripts that are unable to run simultaneously due to resource conflicts are placed in the Waiting queue and execute as soon as the required resources become available. For immediate operations and Backup Set management tasks, Retrospect either asks if you want to wait for the required resource to become available or displays error -843 (resource in use by another operation), in which case you'll have to try again later.

NOTE: Retrospect Professional supports only one execution unit and therefore cannot take advantage of disk Backup Sets' single write/multiple read capabilities.

Configuring Multiple Execution Preferences

You must have more than one execution unit to perform concurrent executions.

See "General Preferences" on page 264 for information on specifying the number of execution units.

WARNING: Retrospect automatically determines the optimal number of execution units based on the backup computer's memory. Override this setting at your own risk.

Assigning Execution Units

You can decide whether you want an operation to use a specific execution unit or the first available execution unit ("Any Execution Unit"). When you have two or more execution units and you create a script or set up an immediate operation, its summary window includes an execution unit list box.
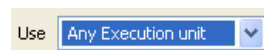
To take advantage of multiple executions, choose "Any Execution Unit". In some cases, you may want executions to run consecutively. For example, you may back up a volume to hard disk, then back up the Catalog File to a CD. In this case, you should assign *the same* execution unit to both operations and schedule the main backup to start before the Catalog backup. This guarantees that the second operation will not execute until the first one is complete.

Multiple Drives

Concurrent executions to multiple tape drives requires Retrospect's Advanced Tape Support add-on. You can perform concurrent executions to multiple stand-alone tape drives, or to tape libraries with multiple built-in drives.

NOTE: Advanced Tape Support is not available for Retrospect Professional or Retrospect Disk-to-Disk.

Binding Tape Backup Sets to Tape Drives

When using multiple tape drives with Retrospect, you may want to "bind" a Backup Set to a specific drive. For example, if you have two tape drives, a faster drive and a slower drive, you may want to bind the Backup Set for your client computers to the slow drive, and the Backup Set for the local server to the fast drive. That way the networking speed and drive speed will be more in sync and the tape drives will have to spend less time repositioning the heads.

By default, Retrospect allows Backup Sets to use any available tape drive, but there are two ways to change this setting:

- You can specify and modify the binding of a tape Backup Set through the Backup Set properties window. Go to Configure> Backup Sets, select a tape Backup Set, and click Properties. In the Properties window, click the Binding tab. Click "Selected tape drives" and select one or more drives. You

can also remove a binding by selecting "Any tape drive".
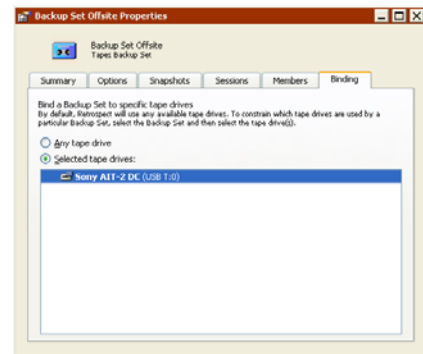
- You can also specify and modify the binding of a tape Backup Set through the Storage Devices window. Click Configure>Devices. In the Storage Devices window, click the Binding tab. Select a Backup Set, click "Selected tape drives," and select one or more drives. You can also remove a binding by selecting "Any tape drive".
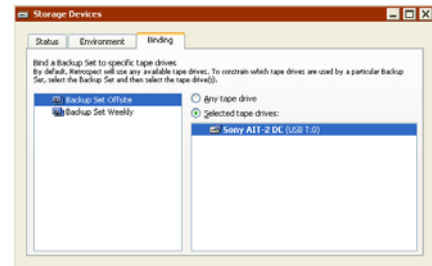
Multiple Tape Drive Strategies

Retrospect Advanced Tape Support (ATS) add-on allows Retrospect to write to multiple tape drives or read and write to separate tape drives at the same time. This allows for more data to be backed up in a given backup window.

The key strategy for maximizing the performance of ATS and meeting your backup window demands is to set up your scripts to stream a unique source to a unique destination, so that multiple operations can run concurrently.

If a specific source or destination is in use by one operation, Retrospect cannot use that source or destination for another concurrent operation.

The following scenarios describe how to structure your scripts and Backup Sets to get the greatest advantage from ATS:

- Scenario 1- Four servers or server volumes to back up to a tape library with two drives
- Scenario 2- A SQL server, Exchange server, file server, and 35 notebooks to back up to a tape library with two drives
- Scenario 3- 500 clients to back up to a tape library with four drives

NOTE: You must have at least two execution units available to run multiple concurrent operations.

Scenario 1- Four servers or server volumes to back up to a tape library with two drives

Without Advanced Tape Support, you would most likely create one script to back up all the servers to a single Backup Set. Since you cannot back up simultaneously to two tape drives without ATS, this is a good option.

With Advanced Tape Support however, you can create two scripts, each of which backs up two servers to a different Backup Set. You can schedule the scripts to run at the same time and back up all the volumes in less time.

Scripts	Script 1 Script 2
Sources	Script 1: Server A and Server B Script 2: Server C and Server D
Destinations	Script 1: Backup Set 1 Script 2: Backup Set 2

Scenario 2- A SQL server, Exchange server, file server, and 35 notebooks to back up to a tape library with two drives

In this example, the servers need to get backed up every night at 10 p.m. and the notebooks need to get backed up as they're available on the network.

Create two scripts, one regular script for the servers and a Proactive backup script for the notebooks.

Scripts	Server Backup Notebook Backup (Proactive Backup script)
Sources	Server Backup: SQL, Exchange, file server Notebook Backup: Notebooks
Destinations	Server Backup: Backup Set 1 Notebook Backup: Backup Set 2
Schedule	Server Backup: 10 p.m., every night Notebook Backup: Always active

This arrangement makes it possible for Retrospect to back up the servers and the notebooks at the same time to different tape drives (as long as the resources are available).

Scenario 3- 500 clients to back up to a tape library with four drives

Organize the clients into four logical groups of a similar size, then create a source group (in the Volumes Database) for each and add the clients.

Create a Backup Set and Proactive Backup script for each source group, then start Proactive Backup.

NETWORKED CLIENTS

- **NETWORKED CLIENTS OVERVIEW**

- **INSTALLING CLIENTS**

- **WORKING WITH CLIENTS**

- **UPDATING CLIENTS**

- **UNINSTALLING A CLIENT AND ITS SOFTWARE**

- **ADVANCED NETWORKING**

- **CLIENT USER PREFERENCES**

- **BACKING UP CLIENTS**

- **WORKING WITH WINDOWS CLIENTS**

- **WORKING WITH MAC OS CLIENTS**

- **WORKING WITH UNIX CLIENTS**

- **WORKING WITH NETWARE CLIENTS**

- **USER INITIATED RESTORE**

- **FILE SYSTEM CONVERSIONS**

- **MICROSOFT NETWORKING VOLUMES**

- **NETWORK BACKUP GUIDELINES**

This chapter provides instructions on installing, configuring, and otherwise administering the client software that allows you to access networked Retrospect client computers from the backup computer. It also describes the options and controls available to Retrospect clients. In addition, this chapter explains how to back up these clients and includes information and worksheets for setting up efficient workgroup backups.

NETWORKED CLIENTS OVERVIEW

Retrospect allows you to use a single computer with a storage device to back up networked Windows, Macintosh, UNIX, and NetWare computers equipped with Retrospect Client software.

The backup administrator—that's you—installs the Retrospect Client software on each of the client computers (also called clients). The backup administrator uses the Retrospect application to log in clients for use by the backup computer. After configuring the clients, the administrator can create and schedule scripts using client volumes as sources, as if the volumes were connected directly to the backup computer.

Client Licenses

Retrospect will work with as many clients as you have licensed. Retrospect Small Business Server, Single Server, and Multi Server support unlimited desktop/notebook clients. You can add licenses to support more desktop/notebook clients with Retrospect Professional.

Retrospect Multi Server supports unlimited server clients. You can add licenses to support server clients with Retrospect Small Business Server and Retrospect Single Server.

Retrospect's License Manager keeps track of your client licenses with the license codes you enter. Client license codes are included with Retrospect and are available separately in Retrospect Clients. You get additional codes when you purchase additional licenses.

- To view current licenses, click Configure> Licenses. The Backup Clients container summarizes the quantities of used and available clients and lists client licenses you have added.
- To add a client license, click the Add button and enter your new license code in the dialog that follows.

- To purchase additional client licenses, click Purchase.

Client licenses are automatically added by the License Manager when you log in previously licensed clients running Retrospect Client software version 4.1 and earlier.

Security

Clients connected to the Internet are at risk, however slight, of unauthorized access. The Retrospect Client installer program requires you to assign passwords (see page 173) to clients to prevent access by Internet users who have Retrospect.

INSTALLING CLIENTS

All client computers that you want to back up must have Retrospect Client software installed. The following topics include system requirements and installation instructions for Windows, Mac OS, UNIX, and NetWare clients.

System Requirements for Windows Client Computers

Windows client computers require:

- Intel Pentium class or better processor
- Windows 95/98/Me, Windows NT 4.0 Workstation or Server (SP6 or greater), Windows 2000 Professional, Server, or Advanced Server (SP2 or greater), Windows 2003 Server, or Windows XP
- TCP/IP networking
- Winsock 2.0 for Windows 95

You can install TCP/IP networking software from the Windows installation software. Windows 95 requires the Winsock 2.0 Update from Microsoft. It is available free from Microsoft at http://www.microsoft.com/windows95/.

NOTE: In order to back up Windows NT 4.0 Server, Windows 2000 Server, Windows 2000

Advanced Server, or Windows Server 2003 computers as Retrospect clients, you must be running Retrospect Multi Server on the backup computer. You can also back up server clients with Retrospect Disk-to-Disk, Small Business Server, or Single Server if you have server client licenses.

Installing Retrospect Client Software on Windows Computers

There are a number of different ways to install Retrospect Client software on Windows computers. The method you choose depends on how you will log in the clients to Retrospect's Backup Client Database. Depending on the number of clients you have and the edition of Retrospect you have, you can either log in clients one by one, or log in multiple clients at one time.

Installing Windows Clients for Individual Log In

If you have a small number of clients, or if you have Retrospect Professional, you can install Retrospect Client for Windows using the Retrospect CD or by copying the client installer files to a network location accessible to the client computers. Individual clients are logged in to Retrospect's Backup Clients Database using the password specified during installation.

Use the following procedure to install the client software on each Windows computer you want to back up over the network.

To Install Windows Clients for Individual Log in:

1. Under Windows NT/2000/XP/2003, log in to the client computer so that you have Administrator privileges.

2. Save all unsaved documents in other running application programs.

3. Insert the Retrospect CD in the client computer's CD-ROM drive.

4. Click the Install Retrospect Client button.

5. Follow the wizard instructions to install the client software.

6. During the installation process, you must enter a password that is used to prevent unauthorized access to the client; do not forget this password.

7. Under Windows NT or 2000, restart the computer.

When the computer starts up it automatically loads the client software. The client is now ready to be accessed from the backup computer, as described in "Working with Clients" on page 171.

TIP: To install clients without using the CD, copy the client installer files to a network location. You can then access these files from each client computer and launch setup.exe to install the software. Using this method, Retrospect Client users can install the software themselves, as long as they make sure to provide their client password to the backup administrator.

Installing Windows Clients for Multiple Log In

In order to take advantage of Retrospect's ability to log in multiple Retrospect for Windows clients at once, including automatic discovery and log in of new clients, you must have Retrospect Disk-to-Disk, Small Business Sever, Single Server, or Multi Server. In addition, if you have Microsoft Systems Management Server (SMS) or Group Policy, you can use these technologies to deploy the client software.

Instead of relying on individual client passwords, multiple client log in uses a private key certificate (on the Retrospect backup computer) and a public key certificate (on each Windows Retrospect Client) to add clients to Retrospect's Backup Client Database. You create these keys in Retrospect, then distribute the public key to the clients using one of the procedures described below.

To Install Windows Clients for Multiple Log In:

1. Copy the client installer files to a network location.

2. Launch Retrospect on the backup computer.

3. Choose Configure>Preferences from Retrospect's navigation bar.

4. Click Clients>Adding.

5. Click Create keys.

6. Enter and confirm a password to protect the private key, then click OK.

Retrospect creates two files, privkey.dat and pubkey.dat at "C:\Documents and Settings\All Users\Application Data\Retrospect".

NOTE: For the greatest security, you should password protect Retrospect, as well as the private key. See "Security Preferences" on page 265.

7. Copy pubkey.dat to the "public_key" folder in the client installer folder on the network.

8. Contact Retrospect Client for Windows users and tell them to launch setup.exe from the client installer folder on the network.

Clients installed this way can be added to Retrospect's Backup Clients Database all at once. See "Adding Clients" on page 171 for more information. Retrospect can even be set up to look for new clients installed this way on a regular basis and add them to the Backup Clients Database automatically. See "Adding Preferences" on page 267 for more information.

To Deploy the Windows Client Installer Using SMS or Group Policy:

1. Launch Retrospect on the backup computer.

2. Choose Configure>Preferences from Retrospect's navigation bar.

3. Click Clients>Adding.

4. Click Create keys.

5. Enter and confirm a password to protect the private key, then click OK.

Retrospect creates two files, privkey.dat and pubkey.dat at "C:\Documents and Settings\All Users\Application Data\Retrospect".

6. Use Microsoft SMS or Group Policy to deploy the Retrospect Client 7.5.msi and pubkey.dat files to multiple clients at once.

NOTE: Client computers must have ISScript 9 and Windows Installer 2.0, both of which are included in the client installer folder on the Retrospect CD, in order to use the .msi file.

Detailed instructions on the use of SMS and Group Policy are beyond the scope of this document. Please refer to those products' documentation for more information on deploying and running installers.

System Requirements for Mac OS Client Computers

Mac OS client computers require:

• PowerPC or greater processor

• Mac OS 7.1 or later with Open Transport 1.1 or later; Mac OS X 10.1.5 or later

• TCP/IP networking

Installing the Client Software on Mac OS Computers

Use the following procedures to install the client software on each Macintosh computer you want to back up over the network.

TIP: For installing many clients on a network from a file server, or for installing on computers without CD-ROM drives, you can make a shared folder on a server with the contents of the Retrospect Clients Installer application. Run the installer program from that folder instead of from the CD.

To Install Retrospect Client Software on a Mac OS Computer:

1. Save all unsaved documents and quit other running application programs.

2. Under Mac OS X, log in to the client computer so that you have administrator privileges.

3. Insert the Retrospect CD in the client computer's CD-ROM drive.

4. Double-click the installer icon to launch the program.

5. Follow the instructions of the installer program to place the client software on the startup disk.

6. Create and enter a password to prevent unauthorized access to the client; do not forget this password.

NOTE: Use only basic alphanumeric characters (low-bit ASCII) in passwords for Macintosh clients. Macintosh high-bit characters do not correspond to Windows high-bit characters. For example, Luf$Luf00 is OK but Lüf•Lüføø will cause problems.

7. Restart the computer.

When the computer starts up, it automatically loads the client software. The client is now ready to be accessed from the backup computer, as described in "Working with Clients".

System Requirements for UNIX Client Computers

The system requirements vary depending on whether the client is running on Linux or Solaris.

Linux client computers require:

- Intel Pentium class or greater processor
- Red Hat Linux, Red Hat Enterprise Linux, SUSE Linux Desktop, SUSE Linux Professional, SUSE Standard Server, or SUSE Enterprise Server operating system (All 32-bit OS only)

Solaris client computers require:

- SPARC-based processor
- Solaris operating system

Both Linux and Solaris clients require:

- glibc version 2 or later
- TCP/IP networking

In order to use the graphical user interface (GUI) to change options and preferences, the following is also required:

- Java version 1.2 or later

NOTE: For a list of current supported versions of Red Hat Linux, SUSE Linux, and Solaris, see the Tqzkq Retrospect web site.

Installing the Client Software on UNIX Computers

Use the following procedures to install the client software on each UNIX computer you want to back up over the network. Choose your preferred method of installation; rpm, pkg, or tar. Where the instructions say *version*, use your specific version/build number of the Retrospect Client software, such as 7.5.103.

To Install Retrospect Client Software on a UNIX Computer:

1. Save all unsaved documents in other running application programs.

2. Log in to the client computer.

3. Insert the Retrospect CD in the client computer's CD-ROM drive and browse to the location of the client installer files.

4. Enter the following commands, respective to your operating system and your preferred installer.

pkg (Solaris only) #pkgadd -d retroc~1.pkg

rpm (Linux only) $rpm -i retroclient-*version*-1.i386.rpm

tar $tar -xf retroclient-version.tar, $.Install.sh

5. Create and enter a password to prevent unauthorized access to the client; do not forget this password.

The client software runs automatically upon completion of installation.

The client is now ready to be accessed from the backup computer, as described in "Working with Clients".

System Requirements for NetWare Client Computers

Retrospect Client for NetWare is supported on NetWare 5.1, 6.0, and 6.5. You must have Retrospect Multi Server, or Retrospect Single Server/Small Business Server/Disk-to-Disk with a server client license, in order to back up NetWare client computers.

NOTE: You cannot back up NetWare clients using Retrospect for Macintosh, or using versions of Retrospect for Windows prior to 7.0.326.

NetWare 5.1 client computers require:

- Service Pack 8
- eDirectory 8.7.3 and above
- Smdr 6.54a
- Smsut 1.01
- TSA500 5.05i
- Dsbk 10510.81.05
- Backupcr 10510.81.05

NetWare 6.0 client computers require:

- Service Pack 5
- eDirectory 8.7.3 and above
- Smdr 6.54a
- Smsut 1.01
- TSAFS 6.50.11
- Dsbk 10510.81.05
- Backupcr 10510.81.05

NetWare 6.5 client computers require:

- Service Pack 3
- eDirectory 8.7.3 and above
- Smdr 6.54a
- Smsut 1.01
- TSAFS 6.50.11

- Dsbk 10510.81.05
- Backupcr 10510.81.05

All versions of NetWare require TCP/IP networking.

Installing Retrospect Client Software on NetWare Computers

Use the following procedures to install the client software on each NetWare computer you want to back up over the network.

To Install Retrospect Client Software on a Netware Computer:

1. Copy the folder "clientpk" and its contents from the Retrospect 7.5 CD to the root of "SYS:" on the NetWare computer.

2. Start the install by typing SYS:clientpk\rtroinst.nlm from the system console.

3. Follow the installer instructions to complete the install. The installer includes a step where you set a password that allows the Retrospect backup computer to access the NetWare client. If you forget this password, you will have to reinstall Retrospect Client for NetWare (see below).

4. Type retroclt from the system console to start the client.

The client is now ready to be accessed from the backup computer, as described in "Working with Clients" on page 171. Repeat the installation procedure for each NetWare client you want to back up.

To Reinstall Retrospect Client for NetWare:

1. Stop the Retrospect Client process by typing retroclt –stop from the NetWare console.

2. Delete the SYS:retroclient directory.

3. Install Retrospect Client for NetWare as described above.

WORKING WITH CLIENTS

Once a client computer is installed with Retrospect Client software, you can add it to the Backup Clients Database from the backup computer and start using it in immediate and automated operations.

Working with Firewalls

When backing up network clients, Retrospect needs certain network access that is not enabled by default with most firewalls.

Retrospect uses port 497 for both TCP and UCP communications. To successfully find and access Retrospect clients, your firewall needs to be set to allow communication over port 497 for both TCP and UDP on all Retrospect clients as well as on the Retrospect backup server.

If you are using the Windows XP SP2 Firewall, Retrospect automatically opens these ports if the firewall is enabled when Retrospect is installed. Otherwise, you must open the ports manually. See your Windows documentation for information on enabling firewall exceptions.

Adding Clients

Before you can back up a client computer, you need to add it to Retrospect's Backup Clients Database. In general, you can only add one client to the database at a time, however under certain circumstances you can add multiple clients at once, and even set up Retrospect to automatically discover and add new clients on your network.

Requirements for adding multiple clients at once:

• Retrospect Disk to Disk, Small Business Server, Single Server, or Multi Server
• Retrospect Client for Windows
• Clients installed with a public key certificate (see "Installing Windows Clients for Multiple Log In" on page 167)

• Multicast or subnet broadcast method of accessing clients

NOTE: When you add a client, Retrospect's License Manager decrements the available pool of client licenses (if applicable).

To Add a Single Client:

1. From the navigation bar, click Configure> Clients.
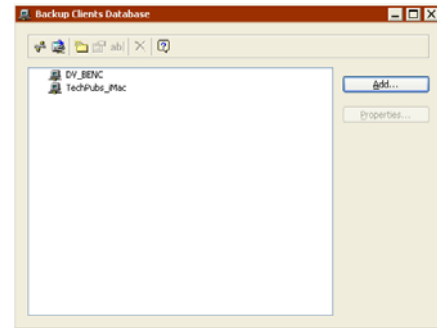
The Backup Clients Database displays a scrolling list of all the client computers currently logged in for use with Retrospect, if any.

2. Click Add to bring up the Live Network window.

This window lists all the computers on a specific network that have Retrospect Client software installed. By default, Retrospect uses its Piton multicast method of searching for clients in the local subnet.

NOTE: A subnet is a group of local computers physically networked together without a router or gateway, though they may use a gateway to connect to other networks.

3. Select a client and click Add.

4. Enter the client's password, then click OK.

Retrospect for NetWare clients display an additional dialog. Enter a user name and password with administrator access to all the volumes on the NetWare computer that you want to back up. If you enter invalid information, you will not be able to see any volumes on the NetWare computer in Retrospect's Volumes Database.

TIP: If you want to log in to the NetWare computer as a different user at somepoint in the future, open Retrospect, choose Configure> Volumes, right-click the NetWare volume in the Volumes Database list, and enter the new user name and password.

Once a client is logged in, the client properties window displays. See "Configuring Clients" for information about client properties.

To Add Multiple Clients:

1. From the navigation bar, click Configure> Clients.
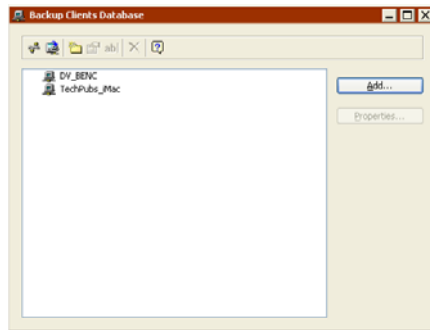
The Backup Clients Database displays a scrolling list of all the client computers currently logged in for use with Retrospect, if any.

2. Click Add to bring up the Live Network window.
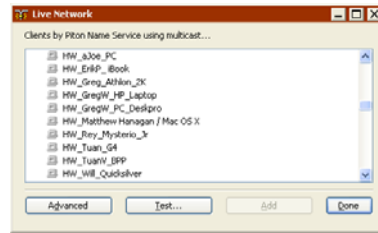
This window lists all the computers on a specific network that have Retrospect Client software installed. By default, Retrospect uses its Piton multicast method of searching for clients in the local subnet.

NOTE: A subnet is a group of local computers physically networked together without a router or gateway, though they may use a gateway to connect to other networks.

3. Select all the clients in the list.

Retrospect automatically deselects non-Windows clients.

4. Click Add.

Clients that have a public key certificate created by the Retrospect backup computer are added. Clients that have a password are not added. Clients that have a public key certificate that was created by a different Retrospect backup computer are not added.

To automatically discover and add clients with a public key certificate and add them to the Backup Clients Database see "Adding Preferences" on page 267.

Testing Network Addresses

You can use the Test button in the Live Network window to test for a responding client at a known IP, DNS, or WINS address.

To Test an Address:

1. From the navigation bar, click Configure> Clients.

2. Click Add to bring up the Live Network window.

3. Click Test.
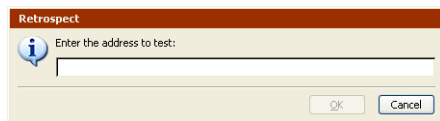
4. Enter an IP, DNS, or WINS address and click OK.

If Retrospect Client software is found at the specified address, Retrospect reports its client name and software version.
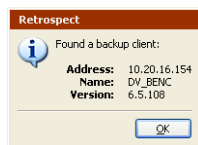
If a computer is found at the specified address, but it is not running Retrospect Client software, Retrospect reports error –541.

If there is no TCP/IP response from the specified address, Retrospect reports error – 530.

The Advanced button accesses Retrospect's advanced networking features, which are described in "Advanced Networking" on page 179.

Configuring Clients

After you have logged in a client, you need to configure it. If a client is already installed but not logged in, you can select it in the Live Network window and click the Add button to log in and configure the client. If the client is already known but you need to reconfigure its settings, you can select it in the Backup Clients Database window and click Properties from the toolbar.

The client properties window is arranged with four tabs:

  • General Tab
  • Access Tab
  • Tools Tab
  • Volumes Tab

General Tab

The General tab shows various information about the backup client and has an option to protect data over the network.
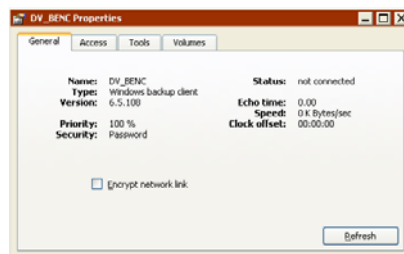
Name is the given client name.

Type indicates the operating system used by the client computer.

Version is the version number of the client software installed on the client computer.

A/C is the activator code of a backup client running 4.1 or older client software.

Priority is the priority setting the user has chosen from the client control panel. A 20% priority means the user has set the slider all the way to "User," giving other applications and tasks some of the computer's processing time that would otherwise be used for Retrospect tasks. A 100% priority means the client's priority slider is set all the way to "Backup," giving client tasks (namely, transferring files) all of the client software's processing time allotted by its operating system.

Security is the data security specified for this client computer:

  • *None* means no password was installed and anyone using Retrospect on the network can log into this client.
  • *Password* means a password must be entered in order to log in to this client.

- *Uses private/public key* means the client does not require a password to be logged in. See "Installing Windows Clients for Multiple Log In" on page 167 for more information.

- *Link Encryption* appears if the client has a password and the Encrypt network link check box is selected. This means data from the client is being encrypted before being sent over the network. You cannot select the Link Encryption option unless you have a password or public/private key.

Status indicates the client's availability for backups and other operations. *Not connected* means Retrospect has not yet established communication with the client. *In use* means the client is presently being accessed. *Connected* means the client is ready and available. *Locked* means the user at this client workstation has checked the "Read Only" access preference in the client control panel. The client can be backed up, but you cannot restore to it or delete files from it. *Busy* means the client is currently being accessed by a different copy of Retrospect on the network. *Turned Off* means the user at this client clicked the "Off" radio button in the client control panel. A client that is turned off is unavailable for operations until it is turned on manually or the client computer is restarted.

Echo time is the time delay, in seconds, experienced in communicating with this client (usually 0.0 to 0.2). If the network or client is busy, or you are using routers, the echo time could easily be higher without indicating a problem.

Speed is the transfer rate of the network connection between the backup computer and the client computer. Click the Refresh button to update Speed information.

Clock offset is the difference in hours:minutes:seconds between the internal clocks of the client computer and the backup computer.

Encrypt network link, which is off by default, is only available if this client uses a password. When the check box is checked Retrospect protects against network eavesdropping by encrypting data transferred over the network then decrypting it before writing it in the Backup Set. (Client link encryption is distinctly different from Backup Set encryption.)

Access Tab

The Access tab summarizes the network access method for this client.
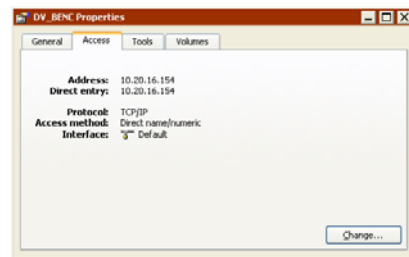
You can click the Change button to access the client in a special Live Network window. This may be necessary if the client has moved on the network or was if it was reinstalled.

Tools Tab

The Tools tab lists the client name, whether it has a password, its clock offset (the time difference between the client computer clock and the clock of the backup computer), and the version number of the client software.

- To change the client name, click Rename. A dialog then asks you to enter and confirm the new name.

- To add or change the password, click Set Password. A series of dialogs then ask you to enter and confirm the new password.
- To add or remove a User Initiated Restore password, click Set UIR Password, then enter and confirm the password. Make sure to provide the password to the Retrospect Client user so they can take advantage of User Initiated Restore (UIR). For more information on UIR, see "User Initiated Restore" on page 191. If this option is disabled, see "User Restore Preferences" on page 268.
- To change the time of the client computer to match that of the backup computer, click Sync Clock, which is not available when the client allows read access only (see page 185).
- To update the software version of the client, click Update. A file selection dialog then asks you to locate the Retrospect Client software from which to update. See "To Update an Individual Client Computer" on page 177 for detailed instructions.

Volumes Tab

The Volumes tab lets you specify which volumes on the client computer are accessible to Retrospect over the network.
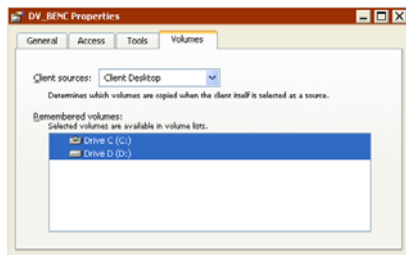
Client sources: The setting of the list box affects how Retrospect resolves client containers during operations. Usually you do not need to change it from its Client Desktop default.

- **Client Desktop** resolves to all volumes local to the client computer, except for floppy disks, shared volumes (such as file servers), read-only volumes (such as CD-ROMs), and empty volumes.
- **Startup Volume** resolves to the volume from which the client computer booted.
- **Selected Volumes** resolves to all volumes selected below in the list of remembered volumes.

Remembered volumes: lists the client's volumes. Only the selected volumes will be available to Retrospect during operations. The selection determines which volumes appear in Retrospect's Volumes Database window. It also determines the volumes to which the client container resolves when the Client sources list box is set to Selected Volumes.

The following table uses the example of a client computer with several mounted volumes. It shows the volumes to which the client container resolves, respective to the different Volumes to Access settings.

These volumes on a client computer…	…with this client sources configuration…	…resolves to these volumes.
Alyosha (C:) Beowulf (D:) Cynics (E:) Drive F (F:) Economics Server	*Client Desktop*	Alyosha Beowulf Cynics
	Startup Volume	Alyosha
	Selected Volumes, with only Beowulf selected in the list of remembered volumes	Beowulf

Forgetting a Client

After a client has been logged in, there may come a time when you no longer need it and its volumes. (For example, a computer is no longer on the network.) In this case, you can tell Retrospect to forget it, which is the opposite of logging it in.

In the Backup Client Database window, select the client and click the Forget button ✕ in the toolbar. Retrospect asks you to confirm this. By clicking OK, you are removing the client volumes from scripts and other lists in Retrospect. This only affects Retrospect on the backup computer in use at the time. It does not affect other copies of Retrospect running on other computers on the network, which remain logged in to the client as usual. Forgetting a client does not affect that client's existing backups.

TIP: You can use Shift+click and Ctrl+click to select and forget multiple clients at once.

Forgetting a client makes one more client license available in the License Manager (see page 166).

UPDATING CLIENTS

There may come a time when you need to update older client software to take advantage of improvements in a newer version. At that time, you can update clients either from the backup computer, or from individual clients.

Updating Clients from the Backup Computer

You can update individual clients as needed, or update all clients of a given type. When you update a client, it retains all of its current settings.

NOTE: It is a good idea to update all clients even if you know some of them are turned off. You can later repeat this operation without affecting the clients that are already updated.

To Update All Clients of a Given Type

From Retrospect's navigation bar, click Configure then click Clients. The Backup Clients Database window appears, listing all client computers currently logged in for use with Retrospect.
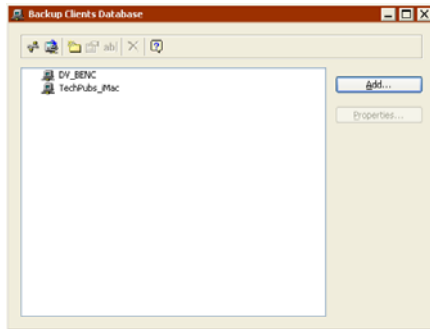
Click the Update clients button in the toolbar. Retrospect asks you to specify the location of the Retrospect Client update (.rcu) file. There are different client update files for different operating systems: Windows, Linux, Solaris, NetWare, Mac OS 7/8/9, and Mac OS X. Different client update files may be available from different places such as the Retrospect CD and the Tqzkq Retrospect web site.

Select the appropriate client update file, wherever it may be, and click Open. After your confirmation, Retrospect begins updating the client software on all client computers of the same type as the selected .rcu file (e.g., Windows, Solaris, etc.). If you have different types of clients, repeat these steps for each type.

NOTE: If a client computer has virus protection software installed, it may require confirmation at the client computer before allowing the update to continue.

When the update is complete, Retrospect reports the results in a dialog and the Operations Log. Click OK.

To confirm the status of each client update, open the Operations Log. (To do this click Reports from the navigation bar then click Operations Log, or choose Operations Log from the Window menu.)

Restart each Mac OS 7/8/9 client computer. The update does not take effect under Mac OS 7/8/9 until the computer is restarted.

Restart each Windows NT 4.0 and Windows 2000 client computer. The update does not take effect on these clients until they are restarted.

For Solaris and Red Hat Linux 6.2 clients, you must manually restart Retrospect Client on each computer with the command:

```
$/usr/local/dantz/client/rcl
start
```

To Update an Individual Client Computer

In the Retrospect navigation bar, click Configure>Clients. The Backup Clients Database window appears, listing all client computers currently logged in for use with Retrospect.

Select the client you want to update then click the Properties button (or double-click the client). In the client properties window that appears, click the Tools tab.

Click the Update button. A dialog appears, prompting you to specify the location of the Retrospect Client update (.rcu) file.

Select the appropriate client update file, and click Open. When the update is complete, another dialog appears, telling you the update completed. Click OK.

The update does not take effect under Mac OS 7/8/9 or Windows NT/2000 until the client computer is restarted. For Solaris and Red Hat Linux 6.2 clients, you must manually restart Retrospect Client on each computer with the command:

```
$/usr/local/dantz/client/rcl
start
```

Updating Clients from the Client Computer

If you do not want to update clients from the backup computer as described above, you can update clients directly from the individual client computers. This is done with the Setup application (Windows), Client Installer application (Mac OS), rpm or tar installers (UNIX), or clientpk (NetWare), which can also update clients.

Follow the installation instructions (see page 166) appropriate for the computer's operating system.

UNINSTALLING A CLIENT AND ITS SOFTWARE

If you want to remove the client software from a computer, forget the client as described in "Forgetting a Client" on page 176, then see the following sections for each type of client:

- Windows
- UNIX
- Mac OS 7/8/9
- Mac OS X
- NetWare

Windows

1. From the Start menu, choose Settings> Control Panel.

2. Double-click Add/Remove Programs.

3. In the window that appears, select the Retrospect Client software and click Change/Remove.

4. Click OK to close the window.

NOTE: Under NT/2000/XP you may have to log in with administrator privileges.

UNIX

The process for uninstalling the UNIX client varies depending on how the client software was installed.

For **rpm**, type the command: $rpm -e retroclient

For **Solaris**, type the command: #pkgrm retroclnt

For **tar**, manually remove the client software files installed by tar.

Mac OS 7/8/9

Remove the Retrospect Client control panel from the computer by placing the file in the Trash.

Mac OS X

1. Open the client installer application.

2. Choose Uninstall from the pop-up menu and select the volume from which to uninstall Retrospect Client software.

3. Click the Uninstall button to remove the client software from the computer, then exit when you are done.

NetWare

1. From the system console, type:
```
unload retroclt
```
2. Delete the entire "Retroclient" directory from the volume (SYS:).

3. Remove the following lines from the SYS:system\autoexec.ncf file:
```
##BeGiN## NetWare NLM required by
Retrospect ###
### Do NOT change anything between
marks, including marks.
Search add SYS:RETROCLIENT\BIN
retroclt
##EnD## NetWare NLMs required by
Retrospect ###
```

ADVANCED NETWORKING

Retrospect normally uses its multicast access method to find backup clients directly connected to the local network segment or local subnet, and display them in the Live Network window. You will need to use Retrospect's more sophisticated techniques of accessing clients if your network has routers between the backup computer and its clients, or if your backup computer has multiple network cards connected to different physical networks.

Retrospect has the ability to use several different methods of accessing clients. It also lets you control the use of adapter cards in the backup computer.

Access Methods

Retrospect can either use the standard DNS and WINS directory services, or its own Piton Name Service based on TCP/IP.

Adding a client to the Retrospect client database also stores its access information for later use. When Retrospect tries to connect to the client for a backup, it resolves the access information into its current IP address using the original access method.

On each client computer, Retrospect Client software waits for queries from Retrospect on the backup computer. Just exactly how Retrospect gets in touch with the clients depends on the access method Retrospect is using.

Multicast

When you first open the live network window, the default access method is multicast. With this method, Retrospect sends out a multicast request to the listening client computers, asking them to respond with their identities. After you have added a client with this method, when Retrospect later tries to connect to the client for a backup, it handles IP address changes automatically by sending out another request to update

its client database and connect with the proper client.

If you use a network analyzer to monitor the packets it sends with the multicast method, you will see Retrospect uses well-known port 497 for its communications. The packet format conforms to the proprietary Retrospect protocol Piton (for PIpelined TransactiONs), which gives Retrospect much of its network speed and reliability. Multicast Piton Name Service uses the assigned address 224.1.0.38, which allows Piton to direct its queries only to those computers running Retrospect Client software.

Multicast access is simple, requiring no configuration, but does not operate across routers. It works only in the local subnet.

Subnet Broadcast

The subnet broadcast access method allows you to access clients through virtually any network topology, including the Internet.

According to TCP/IP standards, every subnet has both a network address and a subnet mask, such as 192.168.1.0 and 255.255.255.0. Routers use these to identify the physical network to which computers are connected. Routers also support queries to all the computers on a particular subnet. Retrospect takes advantage of this ability for its subnet broadcast access method, using the same Piton protocol as for multicast access.

With Retrospect's subnet access method, you must define the address and mask of each subnet you wish to use, and update these configurations if your network changes.

Direct Access

You can use the direct client access method to add a specific backup client to Retrospect's client database. This method requires you to know the IP address or DNS or WINS name of each backup client. Do not use a numeric IP address for computers which get a dynamic IP address

from a DHCP server, because Retrospect has no way to learn when the address changes.

Adding clients by direct access is most useful for a few clients; adding many might be tedious. One of the other methods would probably be better for adding numerous clients.

Configuring Access Methods

The first time you open the Live Network window Retrospect searches for clients in the local subnet using its multicast access method. Click Advanced to access the advanced networking features. The window expands with controls for the network interface and access method.
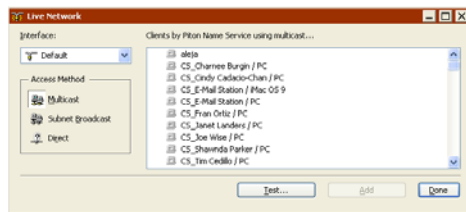
Subnet Broadcast Access Method

You can define other subnets in which Retrospect searches for clients.

Click Subnet Broadcast in the advanced Live Network window to configure a new subnet to search. The first time you use this feature, no subnets are configured so no clients are listed. Click the Subnets button. The first time you do this no subnets are configured, so none appear in the configuration window.
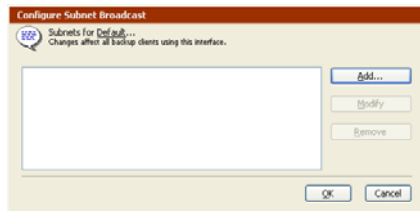
Click Add, and in the dialog that appears, enter an IP address within the subnet and enter its subnet mask. Click OK.

The IP subnet you defined appears in the subnet configuration window.
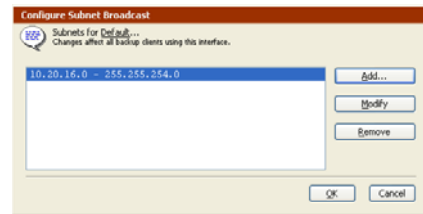
Later, you can add, modify, or remove subnets as needed.

Click OK to return to the Live Network window and view the backup clients Retrospect found using the subnet broadcast access method.
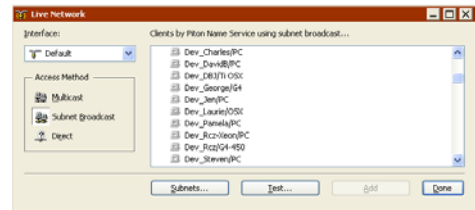
When you add a client with the subnet broadcast access method, Retrospect knows to look for that client in your defined subnets.

Each subnet you configure will be accessed by Retrospect when it searches for clients. This includes not only when this window is open, but also when Retrospect searches for a client in an operation.

NOTE: You can define and use interfaces (see page 181) to limit the number of subnets to search for each client.

Direct Access Method

In the advanced Live Network window, click the Direct access method button. The client list is replaced with an entry box for you to enter the known IP address or DNS or WINS name of a client.
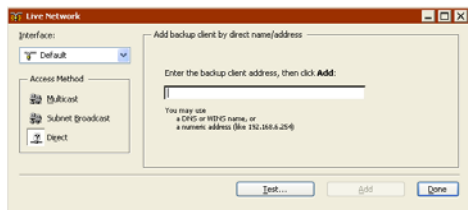
Enter the name or address and click Add. When a client is found at the specified address, Retrospect asks you for its password before logging it into the client database.

NOTE: If Retrospect fails to connect to a client at the specified IP address, see "Client Configuration Issues" on page 310.

After you enter the correct password, Retrospect displays the client's properties window (described in "Configuring Clients," which starts on page 173).

Interfaces

Retrospect's interface feature allows you to choose among multiple adapter cards and control networking options for groups of backup clients. For example, a custom interface lets you back up clients on different subnets without requiring backup data to cross routers, conserving network bandwidth.

Retrospect remembers the interface you used to add a client to the client database, and it will use the interface's settings for all access to that client. You can change the interface used for a client from the client properties window's Access tab.

TIP: To take advantage of a backup computer with multiple NICs when performing multiple concurrent operations, make sure that clients using NIC #1 are backed up to one Backup Set and clients using NIC #2 are backed up to a different Backup Set.

When a TCP/IP-based program such as a web browser initiates a TCP/IP connection, it uses the "default" IP address of the computer to identify itself. Retrospect interfaces let you choose which address to use when your computer has more than one.

Interfaces also allow you to group advanced options. For example, if you want one set of clients to have different timeout values than another set, you can create two separate Retrospect interfaces that both specify the same adapter, but have different timeout settings.

Configuring Interfaces

From the Retrospect navigation bar, click Configure>Clients to display the Backup Clients Database window. Click the Interfaces button on the window's toolbar to open the interfaces window.
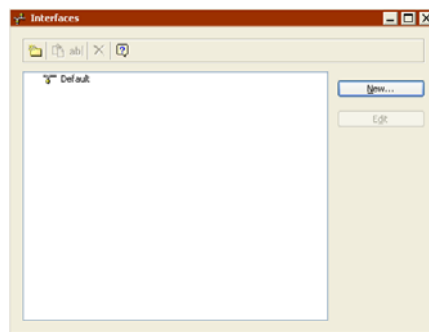
The interfaces window lists the Default interface and any other interfaces you have added.

Adding an Interface: Click the New button and enter a name for the interface and click New. From this point, you are editing the interface as described below.

Editing an Interface: Select an interface in the list and click the Edit button.

NOTE: Do not edit the Default interface until you are completely familiar with the options and their ramifications.
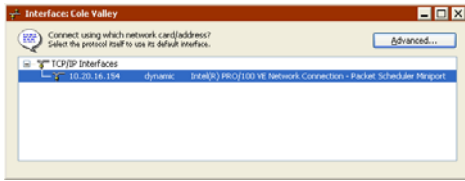
You must first select a TCP/IP interface, usually a network adapter card. It can use a static IP address or one dynamically assigned by a DHCP server. The Default interface always uses the computer's default TCP/IP address and you cannot change it.

TIP: Make sure that Windows is using the fastest network connection as the default for best performance.

Configuring Advanced Options

From the interfaces window, click the Advanced button to open the Advanced Interface Configuration window.
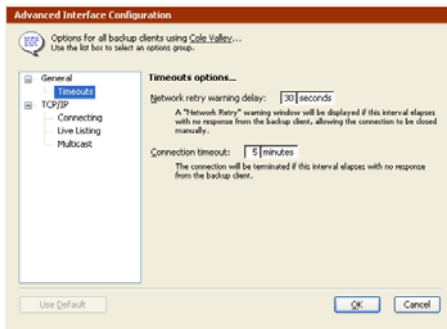
The General options category has options for Retrospect's timeouts.
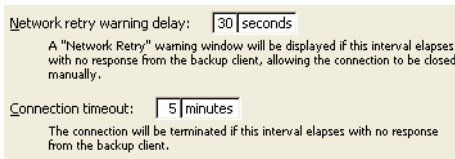
Network retry warning delay: Retrospect displays its network retry dialog when a client does not respond in the specified time period.

Connection timeout: Retrospect terminates an established network connection with a client that does not respond in the specified time period. Retrospect ends the connection and reports error –519 (network communication failed). The operating system's TCP/IP itself might time out sooner, causing error –519 in less time than specified by the general connection timeout. Consider this value the maximum amount of time Retrospect will wait for a client to resume communication.

The TCP/IP options category has options for connecting, live listing, and multicasting.
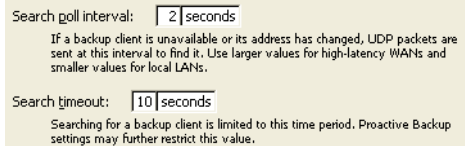
Search poll interval: When a client is unavailable at its last known address, Retrospect sends queries at this interval.

Search timeout: Retrospect terminates its search for a known client when it cannot find the client in the specified time period.

NOTE: This may be further restricted by the Proactive Backup script polling options (see page 237).
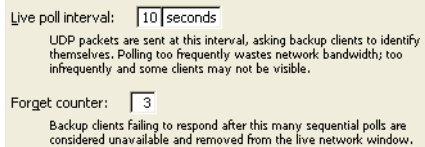
Live poll interval: Retrospect broadcasts to clients at this time interval when it polls for clients in the live network window. If you configured multiple subnets for the interface, Retrospect divides the poll interval by the number of defined subnets.

Forget counter: Retrospect removes a client from the live network window when it does not respond to the specified number of sequential polls. This does not affect clients already added to the backup clients database.

Multicast time-to-live: Retrospect assigns this "time to live" number to multicast UDP packets. It is the maximum number of router hops a packet can make before it is discarded. An increase in the time to live number lets Retrospect search for clients on more subnets connected by IGMP capable routers. Routers which do not support IGMP will not forward the multicast UDP packets.

CLIENT USER PREFERENCES

After the client software has been installed, users of client computers can control some aspects of network backup operations with the Retrospect Client control panel.

NOTE: Retrospect Client for NetWare does not have a control panel. You can manage the NetWare client from the console on the NetWare server using the command line instead. See "NetWare Client Command Line" on page 187 for more information.

You do not need to change any of the settings to perform backups. In most cases, the existing settings are the ones you will want to use. To open the Retrospect Client control panel, do the following:

Windows: From the Start menu, choose Programs>Tqzkq Retrospect>Retrospect Client.

UNIX: Run RetroClient.sh from the installed client folder.

Mac OS 7/8/9: From the menu, choose Control Panels, then open °Retrospect Client.

Mac OS X: From the Applications folder, open Retrospect Client.

The Retrospect Client control panel displays information about the client computer on which it is installed, including the user or computer name, the access status of the client, and a report about the last several backups.
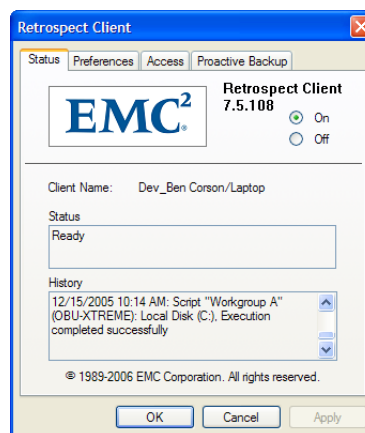
The Windows client control panel, showing the Status tab. (The UNIX client control panel is similar.)
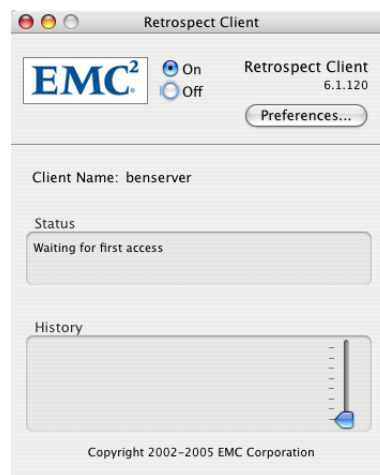
The Mac OS X client application. (The Mac OS 7/8/9 client control panel is similar.)

In addition to the Java-based graphical user interface, UNIX clients can also be controlled through the command line. To see the command line arguments, enter the following.

$retrocpl --help

Access Master Control

The On and Off radio buttons let you allow or deny network access to your client by the backup computer. When you install the client software and each time the client computer starts up, the control is on to allow access. When the control is turned off, the data on the client computer cannot be accessed over the network by Retrospect.

TIP: To permanently prevent access to the client computer, uninstall the Retrospect Client software as described in "Uninstalling a Client and Its Software" on page 178.

General Preferences

The Retrospect Client control panel has additional user preferences for managing client operations. Getting to the preferences is done differently under Windows/UNIX, and Mac OS.

Windows/UNIX: Click the Preferences tab from the four at the top of the control panel.
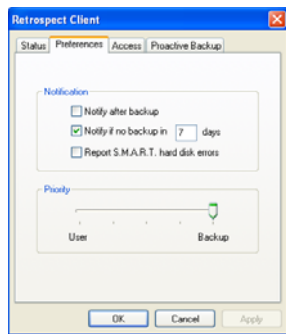
The Windows Retrospect Client control panel's preferences.

Mac OS: Click the Preferences button.
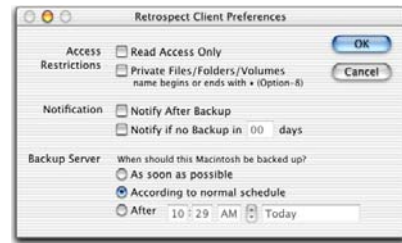
The Mac OS X Retrospect Client control panel's preferences.

Execution Preferences

The execution preference settings allow client users to control how Retrospect interacts with the client computer.

NOTE: These preferences are only available with Mac OS 7/8/9 clients.

Wait at Shutdown determines what happens when a client user chooses Shut Down from the Finder's Special menu. When this option is selected and Shut Down is chosen, the "waiting for backup" dialog is displayed until the backup takes place. By default, this preference is selected.

When this dialog is on the client Macintosh screen, the client user may click Restart to restart the client Macintosh, click Shut Down to shut it down, or click nothing and leave it for unattended operation. When the client computer is not used for thirty seconds, a screen saver appears until the user presses a key or moves the mouse to return to the dialog. When the backup computer finishes its operation with this client, it shuts down the client Macintosh.

Run in Background allows the backup computer to operate at the same time the client user is using the client Macintosh. If the check box is not checked, a dialog appears on the client during network operations. This preference is on by default.

When the dialog appears, the user of the client Macintosh can cancel the network operation to

continue working or wait until the operation is finished. When "Run in Background" is checked, the dialog does not appear during backups, and the client user can set priority levels for local and network operations. See below for details.

Priority Preference

The priority preference allows the client user to make the client computer favor either the user's task at hand or the operation requested by the backup computer. Under Mac OS, this applies only when the "Run in Background" execution preference is on.

NOTE: This preference is not available for the Mac OS X client.

Drag the slider and set it to somewhere in the range between "User" and "Backup." When the slider is set all the way to "User," the computer devotes more of its attention to its user, slowing Retrospect client operations slightly. When the slider is set all the way to "Backup," the client operation is given priority and the client computer is slightly less responsive to its user.

This setting has no effect until the client is actively communicating with the backup computer.

Under Mac OS, the Priority setting is ignored if the client Macintosh is displaying the "waiting for backup" dialog.

Access Restrictions Preferences

These preferences allow the client user to control access to the files and folders on his or her computer.

Read Access Only allows the client computer to be backed up across the network, but prevents writing by the backup computer. This means Retrospect cannot restore, move, or delete files on the client computer, nor can Retrospect be used to rename volumes. The options "Set Volume Backup Date," "Move

Files," and "Synchronize Clock" cannot be used on the client. This setting is off by default.

Private Files/Folders/Volumes makes any files, folders, or volumes designated as private unavailable to the backup computer. This preference is off by default. Select the check box and designate private items as described below.

To designate an item as private under Windows or UNIX, click the Add button, browse to select the item, then click OK or Exclude. Click Add again to exclude more volumes, folders, or individual files. The privacy feature uses the literal pathnames you specify. If you move or rename a file or folder it may no longer be private. If you mount a volume to a different location, its files and folders may no longer be private.

To designate an item as private under Mac OS, type a bullet ("•", Option-8) at the beginning or end of its name (placing it at the end will preserve its sort order in the Finder). For example, you could designate the folder "Personal" as private by renaming it "Personal•".

Notification Preferences

These two preferences allow client users to specify how they are informed about Retrospect network operations.

Notify after Backup directs the client to display a message after the completion of a backup or other operation. The client user can click OK to dismiss the message.

Notify if no Backup in n days directs the client to display a message after 9:01 A.M. if the client has not been backed up within the number of days specified in the entry box. By default, this preference is selected and the number of days is seven.

Report HP Compaq SMART hard drive errors (Windows client only) requests an immediate backup from Proactive Backup (if applicable) when Retrospect learns of errors on

the client's HP Compaq SMART hard drive volumes. By default, this preference is turned on.

Controlling Proactive Backups

There are two ways to control Proactive Backup scripts from the client computer:

- Scheduling from a Client
- Deferring Execution

Scheduling from a Client

If a client is included in a Proactive Backup script, you can use the client control panel to influence when the client gets backed up.

NOTE: Proactive Backup is known as the Backup Server on Mac OS client software.

Mac OS 7/8/9: Click the Schedule button to bring up the Backup Server control dialog.

Mac OS X: The Backup Server preferences appear in the Retrospect Client preferences window.

Windows/UNIX: Click the Proactive Backup tab to bring its controls to the front.
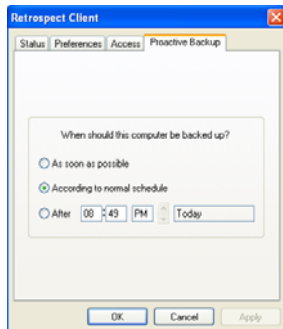
These controls let the user determine when the client computer can be backed up by the backup computer (using a Proactive Backup script). The user would normally use it to initiate a backup or defer a backup, but the user can also revert the Proactive Backup back to its normal

schedule for this client. The Proactive Backup options are:

- **As soon as possible** makes the backup computer back up the client computer as soon as the Proactive Backup is available to do so.
- **According to normal schedule** makes the backup computer back up the client computer at its regularly scheduled time in the Proactive Backup script. (This is the default.)
- **After _____** prevents the backup computer from backing up the client computer before the specified time and date, up to one week from the present time. (Click on the time and date and type or click the arrows to change them.)

Click OK to accept the settings.

Deferring Execution

When Proactive Backup is about to back up a client, a dialog appears on the screen of the client computer.

NOTE: This dialog does not display for NetWare clients.
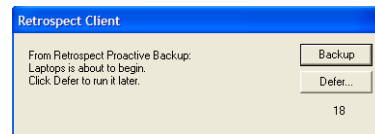
Windows/UNIX client Proactive Backup countdown.
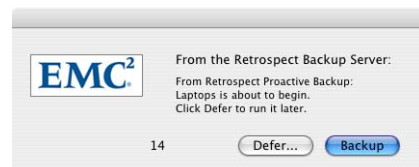
Macintosh client Backup Server countdown.

The dialog gives the client user three ways to control the execution of the impending Proactive Backup operation:

- Waiting for the countdown to reach zero allows the Proactive Client Backup to execute.
- Clicking **Backup** executes the backup immediately.
- Clicking **Defer** lets the user set a later time for the backup to operate.
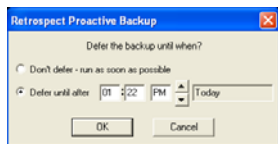
Deferring the Proactive Client Backup from a Windows or UNIX client.
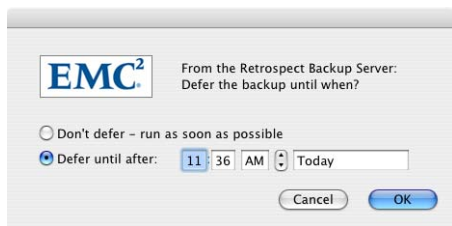
Deferring the Proactive Client Backup from a Macintosh client.

When a user defers, Retrospect makes an entry in the backup computer's Operations Log.

NetWare Client Command Line

Retrospect Client for NetWare does not have a control panel, but you can control many of the same functions using the command line from the NetWare server's console. The following options are available:

`retroclt --help`: Displays a list of client options and parameters.

`retroclt -stop`: Stops the client process.

`retroclt -ip` *n*: Binds the client to a particular IP address (as specified by *n*).

`retroclt -on`: Turns the client on.

`retroclt -off`: Turns the client off.

`retroclt -log` *n*: Sets the logging level, where 0 is no logging and 9 is spew.

`retroclt -readonly [on] [off]`: When readonly is turned on, Retrospect can back up the client, but it cannot write data to the client. This means Retrospect cannot restore, move, or delete files on the client computer.

`retroclt -notifyafter [on] [off]`: When notifyafter is turned on, the client displays a message in the console after the completion of a backup or other operation.

`retroclt -notifyifnobackup [on] [off]`: When notifyifnobackup is turned on, the client displays a message in the console if the client has not been backed up within the number of days specified by notifynumdays.

`retroclt -notifynumdays` *n*: Specifies the number of days; see notifyifnobackup.

`retroclt -exclude [on] [off]`: When exclude is turned on, Retrospect excludes specified files and folders from backups. To exclude files and folders, you must create a file called retroclient.excludes in the retroclient folder on SYS:. The retroclient.excludes file should list the paths you want excluded from backup.

`retroclt -proactive [asap] [normal] [mm:dd:yyyy:hh:mm] [skipdays=`*n*`]`: If the client is included in a Proactive Backup script, you can use this command to influence when the client gets backed up.

- asap makes the backup computer back up the client computer as soon as Proactive Backup is available to do so.
- normal makes the backup computer back up the client computer at its regularly scheduled time in the Proactive Backup script.
- mm:dd:yyyy:hh:mm prevents the backup computer from backing up the client

computer before the specified time and date, up to one week from the present time.

- `skipdays` prevents the backup computer from backing up the client computer for a specified number of days.

BACKING UP CLIENTS

You back up a client volume the same way that you would back up a volume directly connected to the backup computer.

When you set up an immediate or scripted backup, the volume selection window for the source lists available clients under the Backup Clients container and available client volumes under the individual client containers (see page 281).

Backup Clients container
unexposed client container
exposed client container
client startup volume
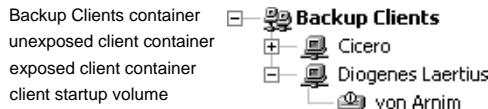
When you set up an immediate backup or make a backup script you have a few different ways of selecting clients and client volumes in the volume selection window for the sources. You can select a client container, one or more specific volumes, or the Backup Clients container. We recommend using client containers or the Backup Clients container. Following are advantages of each method.

Selecting the Backup Clients container selects all individual client containers (described below) logged in at the time of the backup, including new clients you add later.

Selecting a client container selects volumes determined by a client general configuration setting, which is explained in detail in "Volumes Tab" on page 175. Using a client container is simple and maintenance-free, as volumes which are renamed, replaced, or partitioned continue to be backed up with no administrator intervention.

Selecting individual volumes selects only those specific volumes, unlike containers. Retrospect continues to select volumes which are renamed but does not automatically adjust for new, replaced, or partitioned volumes. When the client configuration changes you may need to intervene. This way of selecting volumes is useful, for example, when you do not want to back up all volumes on a particular client. For detailed instructions on selecting volumes, see "Working with Volumes" on page 280.

Selecting folders or groups in your script selects whatever volumes and client containers are placed in the folder or group. This method simplifies script management by allowing you to control your sources in a single place, the volumes database window, available from Configure>Volumes. Using folders in the Backup Clients container lets you better organize a large number of clients. Using groups lets you build lists of volumes and clients which should be backed up together.

TIP: Retrospect Client for Windows computers that were automatically added to the Backup Clients Database using the public key/private key method are grouped in a folder called "Automatically Added Clients" in the Backup Clients container. Enable Retrospect's "Automatically add clients" preference and choose the "Automatically Added Clients" folder as the source for a scripted backup and Retrospect will automatically add new clients to the folder and back them up without requiring any action from the backup administrator. See "Adding Clients" on page 171 for more information, including the limitations of this feature.

WORKING WITH WINDOWS CLIENTS

This section includes tips on using the Windows client, as well as information on its limitations.

If you plan to back up Windows 95 clients, there are certain steps you must take in order to do so.

Fixing Microsoft Windows 95

Two different bugs in Microsoft's network software can cause Retrospect to report networking errors with Windows 95 clients. Microsoft has resolved both problems and free fixes are available for Windows 95. We strongly urge you to update your Windows 95 systems.

NOTE: Windows 98 and Me, Windows NT 4.0, Windows 2000, and Windows XP do not require any updates.

Windows 95 TCP/IP Fix

The hot fix for Windows 95 is installed by the client software Setup program. After installation, choose Run from the Start menu, then type:

C:\Program Files\Retrospect\Retrospect Client\VTCPUPD

(Or type your different installation path.) Click OK. Follow the instructions in Microsoft's installer, then restart to complete the fix. Repeat for each Windows 95 computer.

Windows 95 Winsock Update

Microsoft's Winsock 2.0 update fixes another networking problem present in Windows 95. It is available free from Microsoft at:

http://www.microsoft.com/windows95/
downloads/contents/wuadmintools/
s_wunetworkingtools/w95sockets2/default.asp

Windows System State Backup

Retrospect backs up the Windows system state when Retrospect's option to do so is turned on (see "Windows System Options" on page 244) and the Windows folder is included in the file selection criteria.

Make sure to verify this option in your backups because the system state is necessary for restor-

ing an entire crashed or damaged Windows computer.

Excluded Files

Retrospect excludes certain files from backups and does not show these files in browsers because they cannot or should not be backed up or restored. The files are active virtual memory swap files (.Swp or .Par and Pagefile.Sys) and some client software files.

Open Files

If you have a license code for Open File Backup, you can back up open files on Windows 2000, NT 4.0, and XP client computers.

NOTE: To back up open files on a Windows XP computer, it must have an NTFS volume.

If you do not have Open File Backup, make sure to close open documents and applications on client computers prior to backup.

Screen Savers

For best performance during a backup, do not use a processing-intensive screen saver on a Windows client computer.

WORKING WITH MAC OS CLIENTS

This section includes tips on using the Mac OS client, as well as information on its limitations. Retrospect includes a number of execution options designed specifically for Mac OS clients. See "Macintosh Client Options" on page 249 for more information.

FileVault

Mac OS X 10.3 includes a feature called FileVault. When FileVault is enabled, the entire contents of your Home folder is encrypted and decrypted into a sparseimage file on the fly.

The sparseimage files change constantly and therefore will always get backed up by Progressive Backup. Because of this and because the files can get quite large and under most circum-

stances cannot be restored properly, Tqzkq recommends against enabling FileVault on Mac OS X client computers.

If you must enable FileVault there are a few steps you must take to ensure that all user data is backed up and available for restore:

• Make sure all FileVault users are logged in

• Choose their volumes as backup sources

If the client computer has multiple accounts for users that have FileVault enabled, all those users must be logged in.

In the example above, users with check marks next to their names are logged in.

When they are logged in, their user folders appear in Retrospect's Volumes Database window as separate client volumes. For example, if the FileVault user Chester is logged in, a new volume named "Chester" is listed in Retrospect's Volumes Database window.
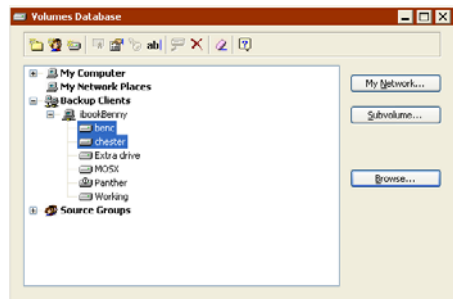
In the example above, benc and chester are FileVault users on the local computer.

In order to ensure that user data is backed up, the FileVault users' volumes must be selected as sources. Selecting the startup disk volume

will not back up the users' data correctly. Selecting the Backup Clients container or a specific client will also select the FileVault volumes it includes.

Sleep Preference

Retrospect cannot wake a sleeping Mac OS client computer to back it up. Make sure that each Mac OS client's sleep preference is set to never put the computer to sleep.

WORKING WITH UNIX CLIENTS

This section includes tips on using the UNIX client, as well as information on its limitations. If you plan to back up UNIX clients, you should be aware of these limitations. Retrospect includes a number of execution options designed specifically for UNIX clients. See "UNIX Client Options" on page 250 for more information.

Excluded Files

Retrospect excludes certain UNIX client files from backups and does not show these files in browsers because they cannot or should not be backed up or restored.

The following types of files are excluded from backup:

• character device crw-------

• block device brw-------

• socket files srw-------

• fifos prw-------

• doors drw-------

File Naming

Linux and Solaris have case-sensitive filenames, which means "myfile" and "Myfile" are considered distinct files. However, Windows, Mac OS, and NetWare have non-case sensitive filenames so "myfile" and "Myfile" are interpreted as the same filename.

If these two files are copied from a UNIX client to a Windows, Mac OS, or NetWare system, they will be named "myfile" and "Myfile-1". When the files are copied back to a UNIX computer, their names will be "myfile" and "Myfile-1".

NOTE: Some Mac OS systems *do* support case-sensitive files names and will copy and restore these files correctly.

WORKING WITH NETWARE CLIENTS

This section includes tips on using the NetWare client, as well as information on its limitations. If you plan to back up NetWare clients, you should be aware of these limitations.

Excluded Files

Retrospect excludes certain NetWare files and directories from backups and does not show these files/directories in browsers because they should not be backed up or restored. The excluded files and directories are:

- SYS:_netware
- SYS:etc\audit.log
- SYS:etc\audit.ctl
- SYS:system\tsa\tsa$temp.*
- SYS: _swap*.mem
- SYS:*.tts
- SYS:SYSTEM\Wanman.log
- SYS:SYSTEM\CSLIB\LOGS\SMLOGS*.tmp
- SYS:LIBDATA\PIPES*.pip
- SYS:SYSTEM\CertServ\KMOCache
- SYS:etc\Volmn
- SYS:etc\Logcache

USER INITIATED RESTORE

User Initiated Restore (UIR) is available as an add-on product for Retrospect. It allows Retrospect Client users to restore their own files from recent hard disk backups, without having to involve the backup administrator. Once UIR is set up, Retrospect Client users can access a web page from their computers and see a list of files available to restore. Users can then restore any of those files back to their own computer. The Retrospect backup administrator can log into the web page and restore files from any Retrospect Client to any other Retrospect Client.

Files are restored to a new folder at a location specified during the restore. No files are overwritten, although the restored files can be moved to any location.

There are some limitations to User Initiated Restore:

- The only files available to restore are those in disk Backup Sets stored on a hard drive accessible to the Retrospect backup server. UIR is not supported with other Backup Set types.
- Only files from *active* Snapshots can be restored. The number of active Snapshots depends on the Backup Set's grooming settings and whether or not any Snapshots have been retrieved or locked. Generally, active Snapshots represent the most recent backups.
- Users can only restore their own files back to their own computer.

NOTE: UIR is best-suited for restoring documents. If you need to restore an entire computer (including its System State) or roll back an application, the backup administrator should perform an immediate restore from the Retrospect backup server. See "Restore" on page 69 for more information.

Requirements for User Initiated Restore

There are UIR requirements for both the Retrospect backup computer and the Retrospect Client computer.

Backup Computer

The backup computer requires:

- Server-level version of Retrospect (Multi Server, Single Server, Small Business Server, or Disk-to-Disk)
- Any supported Windows operating system, except Windows 98, Windows Me, or Windows NT 4.0.
- License for the User Initiated Restore Add-on
- Microsoft Internet Information Services (IIS) installed and running on the backup server
- Microsoft .NET Framework 1.1 or later
- A hard drive or network drive to use as the destination for Retrospect Client backups

TIP: The IIS server should use HTTPS, SSL, or equivalent encryption to ensure all communication is secure.

Client Computers

User Initiated Restore only supports Retrospect Client for Windows, Mac OS X, and Linux. Retrospect Client for NetWare, Solaris, or pre-Mac OS X are *not* supported.

Retrospect Client for Windows supports the following browsers:

- Microsoft Internet Explorer 6.x or later
- Mozilla Firefox 1.x

Retrospect Client for Macintosh OS X supports the following browsers:

- Safari 1.3 or later
- Mozilla Firefox 1.x

Retrospect Client for Linux supports the Mozilla Firefox 1.x browser.

In general, you should always run the latest version of Retrospect Client. UIR *is* supported with older versions of Retrospect Client for Windows, Linux, and Mac OS X, although these clients do not support UIR passwords. See "User Restore Preferences" on page 268 for more information on UIR passwords.

NOTE: User Initiated Restore is not supported on clients set up for read access only.

Installing User Initiated Restore

Before installing UIR, you must install the following components on the Retrospect backup server:

- Retrospect 7.5 (Multi Server, Single Server, Small Business Server, or Disk-to-Disk)
- Microsoft Internet Information Services (IIS)
- Microsoft .NET Framework 1.1 or later

To install UIR:

1. Launch Retrospect.

2. Choose Configure>Preferences from Retrospect's navigation bar.

3. Click Clients>User Restore.

4. Click Install UIR.

This launches the User Initiated Restore Setup Wizard.

5. Follow the onscreen prompts to complete the installation.

NOTE: By default, UIR is installed to an IIS virtual directory named "myrestore" running on TCP port 80. If you change these settings during installation, make sure you provide Retrospect Client users the correct information about how to connect to the UIR web site.

Setting Up User Initiated Restore

Once you have installed all the UIR components, you can launch Retrospect and set it up for UIR, then notify Retrospect Client users to let them know how to access and use UIR.

Setting Up UIR in Retrospect

To set up UIR:

1. Launch Retrospect.

2. Choose Configure>Licenses from Retrospect's navigation bar.

If the License Manager shows a license for User Initiated Restore, skip to the next step. Otherwise, click Add and enter your UIR license code.

3. Choose Configure>Preferences from Retrospect's navigation bar.

4. Click Clients>User Restore.

5. Select the "Enable User Initiated Restore" check box.

6. If you want to require users to enter a password in order to access UIR, select the "Require password for User Initiated Restore" check box.

If you enable this option, you will have to enter a password for each client from the Tools tab in the Client Properties window. See "Tools Tab" on page 174 for more information. You can also select multiple clients in the Backup Clients Database then right-click the selection and choose Set User Restore Password. In this case, all selected clients will have the *same* UIR password.

NOTE: If you want to require a UIR password, you must update all your Windows, Linux, and Mac OS X clients to the latest Retrospect Client software. Although UIR *is* supported with older versions of Retrospect Client for Windows, Linux, and Mac OS X, these clients do not support UIR passwords and they cannot use UIR if a password is required.

7. Enter an e-mail address for the backup administrator and notes to users in the appropriate text boxes.

This information will be available to users from the UIR web page.

8. Click Execution>Security.

9. Click the Protect button.

10. Enter a password for Retrospect and click OK.

NOTE: This is only required for *administrator* UIR. When the administrator accesses the UIR web page, they must enter this password, at which point they can access backups for all Retrospect Clients.

11. Click OK.

Now that UIR is set up, you'll need to let users know how to access it.

If you have already been backing up Retrospect Clients to hard disk with an earlier version of Retrospect, the active Snapshots for those backups will be available from UIR immediately. If you have not used Retrospect before, set up an immediate or scripted backup that copies data from Retrospect Clients to a hard drive disk Backup Set. After the backup, Retrospect Client users will have access to their data through UIR.

Notifying Users About UIR

Once UIR is set up and there are Retrospect Client backups available from which to restore, you should notify users that UIR is available and provide them with information about how to access and use this feature. In order to take advantage of UIR, Retrospect Client users will need to know:

• The URL for the UIR web page: The default URL is http://*ComputerName*/myrestore, where *ComputerName* is the DNS name or IP address of the Retrospect backup server. If you changed the name of the IIS virtual directory or port number during installation,

you will need to modify the default URL to account for any changes.

- The UIR password: If you selected the Retrospect preference requiring a password for UIR and set a UIR password for each Retrospect Client, you will need to provide each client user with their password.

- Information about when to use UIR: UIR is best-suited for restoring documents. If users need to restore their entire computer (including its System State) or roll back an application, they should contact the backup administrator and have him perform an immediate restore from the Retrospect backup server.

- Retrospect backup administrator contact information: You should provide users with a way to contact the backup administrator if they have questions or problems with UIR. This information can also be entered into the appropriate fields in the Clients>User Restore preference and accessed by clicking the "Need assistance?" link from the UIR web page.

TIP: You should only notify client users running Retrospect Client for Windows, Linux, or Mac OS X, since those are the only clients that support UIR.

Restoring with User Initiated Restore

User Initiated Restores can be performed either by a Retrospect Client user or by the Retrospect backup server administrator. The difference is that the user only has access to his or her own files, while the administrator has access to the files of all Retrospect Clients.

NOTE: UIR is best-suited for restoring documents. If you need to restore an entire computer (including its System State) or roll back an application, the backup administrator should perform an immediate restore from the Retrospect backup server. See "Restore" on page 69 for more information.

For UIR troubleshooting information, see "User Initiated Restore Issues" on page 318.

Retrospect Client UIR

In order to prevent unauthorized access to files belonging to other users, there are certain requirements for client UIR:

- Users can only access the UIR web page from their own computer
- Retrospect Client must be running

TIP: The best way to prevent unauthorized access to users' files is to set a UIR password for each client.

Since User Initiated Restore needs to access the Retrospect backup server in order to successfully restore files, there are some additional requirements for the backup server:

- Retrospect must be running on backup server
- Retrospect must have an available execution unit
- The hard drive containing the backups must be accessible to Retrospect

To restore files using Client UIR:

1. From the Retrospect Client computer, launch a supported web browser (see "Client Computers" on page 192).

2. Enter the URL for the Client User Initiated Restore web page.
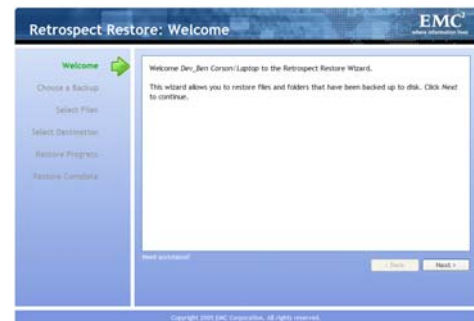
The backup administrator should provide this URL to all users. The URL generally takes the form of: http://*ComputerName*/myrestore, where *ComputerName* is the DNS name or IP address of the Retrospect backup server.

3. If the administrator chose to require a password, enter it in the Welcome screen and click Next.

TIP: To change the password assigned by the backup administrator, click Change Password, enter the old password, then enter and confirm a new password.

4. Choose a backup from the list and click Next.
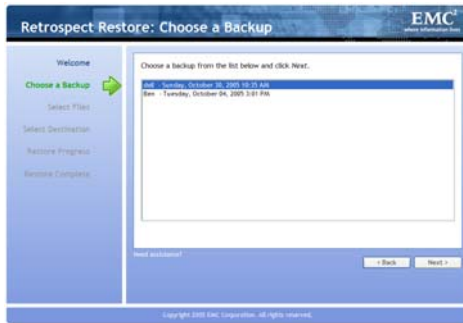
The list generally includes only the most recent backups. If you need to restore files from an earlier backup that is not available, contact the backup administrator. Click the "Need assistance?" link for information provided by the administrator.

5. Select the files and folders you want to restore and click Next.

TIP: If you want a quick way to find files in a backup, you can enter search terms in the Find text box, the click Find. The list of files is filtered to show only those files that match your search criteria. Click Clear to clear your search and display all files and folders again. UIR Find supports the asterisk (*) and question mark (?) wildcard characters.

6. Select a location for the restore.

By default, restored files and folders will be copied to a folder (named after the Backup Set) inside the folder "My Restored Files" at the root of the client computer. For example, C:\My Restored Files\Backup Set A.

7. Click Next to begin restoring.

8. After the files are successfully restored, close the browser window and navigate to the location of the restored files.

Administrator UIR

Administrators can access UIR web page from any computer, regardless of whether or not Retrospect Client is installed on it. The administrator can restore files from any supported Retrospect Client to any other supported Retrospect Client as long as the following requirements are met:

- Retrospect must be password protected (see "Security Preferences" on page 265)
- Retrospect must be running on backup server
- Retrospect must have an available execution unit
- The hard drive containing the backups must be accessible to Retrospect
- Retrospect Client must be running on the computer to which files are being restored

To restore files using Administrator UIR:

1. Launch a supported web browser (see "Client Computers" on page 192) from any computer.

2. Enter the URL for the Administrator User Initiated Restore web page.

The URL generally takes the form of:
http://*ComputerName*/myrestore/default.aspx?
admin, where *ComputerName* is the DNS name
or IP address of the Retrospect backup server.

3. Enter the password in the Welcome screen
and click Next.

4. Choose a client and a backup that contains
the files you want to restore and click Next.

The list includes only the most recent backups.
If you need to restore files from an earlier
backup, you can use Retrospect to retrieve older
Snapshots then restore using UIR, or restore the
files using Retrospect instead of UIR.

5. Select the files and folder you want to
restore and click Next.

6. Select a location for the restore, including
the Retrospect Client name and path.

By default, restored files and folders will be
copied to a folder (named after the Backup Set)
inside the folder "My Restored Files" at the root

of the client computer. For example, C:\My
Restored Files\Backup Set A.

7. Click Next to begin restoring.

8. After the files are successfully restored,
close the browser window and contact the
Retrospect Client user to let him know the
location of the restored files.

FILE SYSTEM CONVERSIONS

Retrospect allows you to restore and duplicate
data between computers that use different oper-
ating systems and file systems. Because no two
file systems support identical attributes and file
formats, copying files from one file system to
another sometimes results in the loss of
information.

Retrospect supports the following file system
conversions with no loss of data:

- FAT (Windows) to HFS (Macintosh)
- FAT to NTFS (Windows)
- HFS to NTFS
- FAT to UNIX file systems
- UNIX to HFS (Mac OS X only)
- FAT to NetWare file systems
- NetWare to HFS (Mac OS X only)

Retrospect supports the following file system
conversions with loss of extended information
and/or data, as noted:

- HFS to FAT: Data fork of HFS files is
  copied; attributes, privileges, and resource
  fork are not.
- NTFS to FAT: First data stream is copied,
  but all permissions and other NTFS data are
  not.
- NTFS to HFS: Services for Macintosh data
  on an NTFS volume restores or duplicates
  without loss to Macintosh HFS volumes.
  When copying Windows NTFS data to HFS

the first data stream is copied, but all permissions and other NTFS data are not.

- NTFS to UNIX: Lose permissions and other NTFS data.
- UNIX to HFS (Mac OS 9.x): Lose UNIX file permissions, owner and group attributes, and special file attributes (e.g. hard links).
- UNIX to FAT: Lose UNIX file permissions, owner and group attributes, and special file attributes (e.g. hard links).
- NTFS to NetWare: Lose permissions and other NTFS data.
- NetWare to HFS (Mac OS 9.x): Lose NetWare file permissions, owner and group attributes, and special file attributes.
- NetWare to FAT: Lose NetWare file permissions, owner and group attributes, and special file attributes.

NOTE: Mac OS file names can include several characters Windows does not allow in its file names. These illegal characters are /, \, :, *,", <, and >. When restoring or duplicating Macintosh files to a Windows volume, Retrospect replaces each of these illegal characters with a hyphen (-).

MICROSOFT NETWORKING VOLUMES

If you want to set up unattended backups through Microsoft Networking instead of through Retrospect Client software, you must run Retrospect as a user that has permissions for the volumes. See "Security Preferences" on page 265 for more information.

To add a network volume to the Volumes Database see "My Network Places" on page 282.

WARNING: Retrospect does not back up the registry and System State when you back up a Microsoft Networking volume this way. Install Retrospect Client software on the computer and use it as a client of Retrospect to back up its registry and System State.

NETWORK BACKUP GUIDELINES

This section provides information, advice, and worksheets to help you set up a workgroup backup using Retrospect.

In general, the same principles that apply to individual backups also apply to network backups of client computers. The major difference between an individual backup and a network backup is the amount of data, which may overwhelm storage limitations. As a consequence of the sheer amount of data and the often slower speed of network backups, time may also impose limitations. If you cannot back up the entire network in a single night, you may want to consider splitting the backup over several nights, backing up only documents, or using Proactive Backup scripts.

Although the information in this section can be applied to any local area network, the examples assume a basic Ethernet network installation. Most calculations will still apply if your network contains inter-network devices (such as routers or gateways), unless one or more members of the backup workgroup are separated from the rest by an inter-network device. Running backups through routers or gateways increases the time it takes to complete a backup.

Choosing the Backup Device

The capacity of the backup device is usually the most important consideration for automatic, unattended workgroup backups. There is no such thing as too much capacity for network backups. More capacity almost always means you can back up more files from more volumes from more client computers, broaden the criteria for selecting files to be backed up, increase the amount of time between media changes, and in-

crease the number of backup sessions per piece of media.

If your backup device does not have enough capacity, you will not be able to complete an automatic, unattended backup because you will have to change the media before the backup is finished.

Choosing the Backup Computer

This section offers some advice on how to select the correct backup device and backup computer to suit your planned network backups.

You need not use a file server as the backup computer. Table 7-1 below lists various advantages of using a desktop computer or a server as the backup computer.

Although the backup computer can be virtually any Windows-compatible model, consider using a computer with adequate power to perform your network backups. For example, if you are backing up a small number of client computers with small to medium capacity hard disks, a 400 MHz Pentium should be able to do the job. However, if you are backing up large file servers and several client computers with thousands of files, a Pentium 4 would be more suitable. Following are some considerations.

The performance of the backup computer often determines the performance of the entire system. Generally, a higher performance computer supports a network backup of more data from a larger number of client computers.

Software compression and encryption increase CPU use significantly. If you are considering using either of these features, choose a model with a more powerful CPU, such as a Pentium IV.

Make sure the backup computer has enough RAM to handle the network volume that contains the most files. The more files you have, the more RAM you need.

If the backup computer is not completing backups in its scheduled time periods or if you want volumes to be backed up more often than they are, you may need a faster backup computer or a faster backup device, or both.

See "Managing Resources," which starts on page 142 for more information.

Advantages of Desktop	Advantages of Server
• You can use the computer closest to you for easy access to the tape drive and Retrospect. • Avoids expense of a dedicated server. • You can select the computer best suited in terms of memory and speed. Retrospect can be run at night or on weekends, allowing normal use of the computer during work hours. • Allows your server to run at full speed for those who are accessing it while the backup is running.	• Optimizes your backup speed since servers are often a high performance model. • Takes advantage of the server's inactivity during the nights and weekends. • Gains added security for your Backup Sets if your server is located in a secure area. • Backs up large server disks using faster local transfer rates rather than the slower network transfer rates.

Table 7-1: Advantages of using a desktop computer or a server as the backup computer.

Encryption and Compression

Retrospect provides an encryption feature that lets you protect your data from unauthorized access as it is being backed up, and a compression feature that saves space on the backup device by compressing stored data. The decision to use one or both of these features can affect the type of backup device you choose. Keep in mind Retrospect's encryption and software compression will slow backups, especially when using a computer with a slow CPU. A tape drive that supports compression will perform the task of compression itself, because it compresses data faster than Retrospect. Use the following table to determine whether to use compression and encryption and whether a compression tape drive is appropriate to use as the backup device.

Feature	Description	Procedure	Implementation
Compression	Allows the backup device to store more files on its media.	Finds patterns in the data; the more patterns, the greater the compression.	If you have a compression drive, Retrospect leaves the task of compression to the hardware since it compresses data faster than Retrospect.
Encryption	Adds security to your backup.	Randomizes the appearance of data to prevent unauthorized access.	Retrospect always manages encryption.
Compression with encryption	Allows the backup device to store more files on its media and adds security to your backup.	Compression must take place before encryption.	Retrospect must perform both functions. If you have a compression drive, you must choose between using encryption or using hardware compression because you cannot use both. (Retrospect automatically disables hardware compression when you use encryption.)

Device Capacity Worksheet

Use this worksheet to estimate the minimum required capacity of a backup device for your workgroup. The number you come up with for *G* is the minimum backup device media capacity for completing an unattended backup without having to change the media.

Item	Description	Amount
A. Total disk capacity *user-defined*	On a separate page, list your workgroup's computers and the disk size (in megabytes) of each. Work out the sum and enter it for *A*.	$A =$
B. Estimated data redundancy *user-defined*	Estimate how much data is redundant, which Retrospect backs up only once. If everyone in your workgroup uses the same applications, dictionaries, fonts, and so on, you might have as much as 60% (0.6) redundancy. If your network is average, enter 0.3 for 30%. Enter your estimate of the redundancy percentage *B,* expressed in decimal form.	$B =$
C. Reduction factor $C = 1 - B$	Subtract the amount *B* from 1 to get the data reduction factor. For example, if *B* is 0.3 the reduction factor is 0.7 (because $1 - 0.3 = 0.7$). Work out the difference and enter it for *C*.	$C =$
D. Reduced data $D = A * C$	To estimate the actual amount of data you need to back up (before any compression) multiply the total disk capacity *(A)* and the reduction factor *(C)*. Work out the product and enter it for *D*.	$D =$
E. Estimated compression *user-defined*	The compression rate depends on the files. Text files compress well; application files do not. The most compression you can hope for is 50% (0.5). Average compression to expect for network backups is 30% (0.3). If you do not plan on using compression, enter 0. Enter your estimate of the compression percentage *E,* expressed in decimal form.	$E =$
F. Compression factor $F = 1 - E$	Subtract the estimated compression *(E)* from 1. For example, if *E* is 0.30 (30%) then *F* is 0.70 (because $1 - 0.30 = 0.70$). Work out the difference and enter it for *F*.	$F =$
G. Required backup capacity $G = D * F$	To get the minimum required backup device capacity multiply the reduced data amount *(D)* by the compression factor *(F)*. Work out the product and enter it for *G*.	$G =$

Backup Duration Worksheet

Once you have determined the size of your backup device, use the worksheet below to determine the number of hours your network backup requires. If the total number of hours is less than twelve, a Recycle backup is likely able to complete in a single night. If the total number of hours is more than twelve, you may need to examine alternative strategies, such as performing Recycle backups only on weekends or backing up only documents and preferences.

Alternative strategies are suggested in "Backup Strategies" on page 224.

Item	Description	Amount
H. Backup capacity requirement $H = D$	For *H,* enter the total reduced data requirement from item *D* in the Device Capacity Worksheet.	$H =$
I. Verification multiplier *user-defined*	If you do not plan to use verification enter 1. For Thorough verification, start with 1.7, for Media verification, start with 1.2. If you are using software compression or encryption, increase it by 0.1 to 0.5; the slower the backup computer, the higher the number. Enter your verification multiplier for *I.*	$I =$
J. Total transmission $J = H * I$	To get the total amount of data transmitted across the network multiply the backup capacity requirement *(H)* by the verification multiplier *(I).* Work out the product and enter it for *J.*	$J =$
K. Network throughput *user-defined*	Throughput rates vary according to the network cabling method. For 10BaseT, use 2400 MB per hour; for 100BaseT, use 9600 MB per hour. Enter the number of megabytes per hour for *K.*	$K =$
L. Adjusted network throughput $L = K \, (1 - .05n)$	Backing up through routers typically reduces performance so subtract 5% for each router. (Use *n* as the number of routers.) Work out the difference and enter it for *L.* If you are not using routers or bridges assign the *K* value to *L.*	$L =$
M. Hours required $M = \dfrac{J}{L}$	To determine the total number of hours required for the backup to complete divide the total transmission *(J)* by the adjusted network throughput *(L).* Work out the result and enter it for *M.*	$M =$

DISASTER RECOVERY

- **OVERVIEW OF DISASTER RECOVERY**

- **PREPARING FOR DISASTER RECOVERY**

- **RESTORING THE BACKUP COMPUTER**

- **RESTORING CLIENT COMPUTERS**

This chapter describes how to prepare for disaster recovery and how to restore local and client computers when disaster strikes.

OVERVIEW OF DISASTER RECOVERY

Retrospect has tools and features to help you prepare for and recover from a disastrous data loss in which the computing environment required to restore that data is not available. If you can boot your computer and start Retrospect, you can use the application's restore function as described in "Restore," which starts on page 69.

Depending upon the edition of Retrospect that you have and the license codes you have purchased, you may have the ability to create a bootable disaster recovery CD for the backup computer and/or Windows client computers.

To check your licenses, click Configure>Licenses. If Disaster Recovery is listed, double-click the certificate icon to learn whether you can create Windows client disaster recovery CDs.

NOTE: Retrospect Professional does not support client disaster recovery CDs. Retrospect does not support client disaster recovery CDs for Windows 95 or Windows NT 4.0 clients.

All editions of Retrospect can use the Prepare for Disaster Recovery wizard to create a custom set of instructions for restoring the backup computer.

PREPARING FOR DISASTER RECOVERY

Retrospect's Prepare for Disaster Recovery wizard helps you create a set of custom instructions and/or a disaster recovery CD that will help you get up and running again if disaster strikes.

A disaster recovery CD provides a quick and automated method to recover the data from the backup computer and Windows clients (depending on your license and the client OS).

If your copy of Retrospect does not have the ability to create a disaster recovery CD, you can still restore files and computers manually, using the instructions generated by the wizard, or those included here.

The end product of the wizard, depending on your selections, is either text instructions or a combination of instructions and a CD image. You can save the instructions as a text file or print them from the wizard. The instructions are also saved in a text file in the CD image. The CD image is saved as an ISO 9660 format image file. You can use this image file with your favorite CD mastering software and a CD/DVD drive to "burn," or record, a Disaster Recovery CD.

NOTE: Nearly all CD/DVD drives include mastering software and documentation on how to burn a CD from an ISO image.

Using the Wizard

Before you use the Prepare for Disaster Recovery wizard, you must perform a complete backup of the computer's startup volume and any other hard disks or partitions you want to restore after a disaster.

See Chapter 4 • Immediate Operations for more information on backing up.

NOTE: Use the All Files selector or the All Files Except Cache Files selector with your backups to ensure the computer can be completely restored after a disaster.

Once you have a complete backup of the computer's startup volume, you can use the Prepare for Disaster Recovery wizard to create instructions or a CD-R disc image.

To Prepare for Disaster Recovery:
1. Starting
Choose Backup>Disaster Recovery from Retrospect's navigation bar. This opens

Retrospect's Disaster Recovery preparation wizard.

2. Selecting the Snapshot
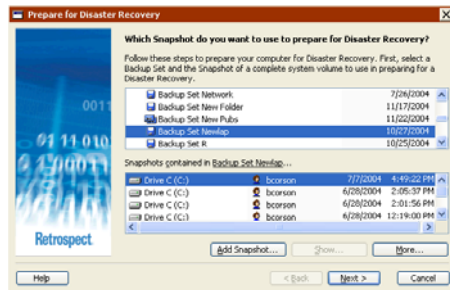
The wizard asks you to select a Backup Set and Snapshot. Select the Snapshot from the most recent complete backup of the system volume (the disk Windows starts from). The Snapshot does not have to be of the computer you are using; you may select a system volume Snapshot of any computer backed up with Retrospect.

The following table summarizes Retrospect's available Disaster Recovery options for the selected volume Snapshot.

Selected Snapshot	Available Disaster Recovery Preparation
local Windows system volume	bootable CD image or instructions
client Windows system volume	bootable CD image (if license is available and client is not Windows 95 or Windows NT 4.0) otherwise instructions only
non-system Windows volume	none
non-Windows volume	none

Click Next to proceed.

3. Selecting the Wizard Output

The preparation wizard asks whether you want to create a CD-R disc image or text instructions only.
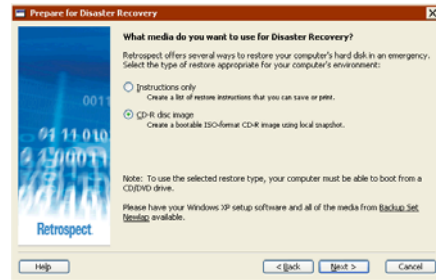
If you can select CD-R disc image, you will be able to create a CD that you can later use to boot and restore the computer from the selected Snapshot. If CD-R disc image is not available, choose Instructions only.

Make your selection and click Next to proceed.

4. Entering Windows Authentication Code

The preparation wizard may ask for your Windows product ID or key. Carefully enter the code from the label on your Microsoft certificate of authenticity and click Next to proceed.

If you are preparing instructions only skip ahead to step 8.

If you are preparing a CD-R disc image for a Windows 98 or Me computer, skip to step 6.

5. Locating Windows NT/2000/XP Installation Software

If you are preparing a CD-R disc image for a Windows NT/2000/XP computer, the preparation wizard next asks you to locate the Windows installation software.

Insert the Windows installation CD and select the txtsetup.sif file within the i386 folder.

NOTE: Some computers do not include a Windows installation CD, but do have the i386 folder on the hard drive. In this case, browse to the i386 on your hard drive and select the txtsetup.sif folder there.

6. Specifying a Location to Save the CD Image

The preparation wizard next asks where you want to save the CD image file.

The wizard shows the path where the CD image file is to be saved. Click the Browse button if you wish to choose a different location.

Click Next to proceed.

7. Building the Image

The preparation wizard begins building a CD image.
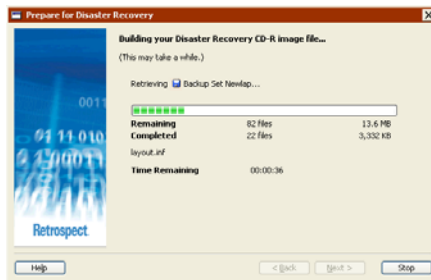
The wizard copies needed files from the local hard disk, if they are available there, and from the Backup Set media. (You may be prompted to insert one or more members of the Backup Set. Have the media ready.)

After gathering the needed components, Retrospect saves an ISO format image file. You can later use this image file with your favorite CD mastering software and a disc drive to "burn" a Disaster Recovery CD.

8. Finishing

The wizard's final window appears.
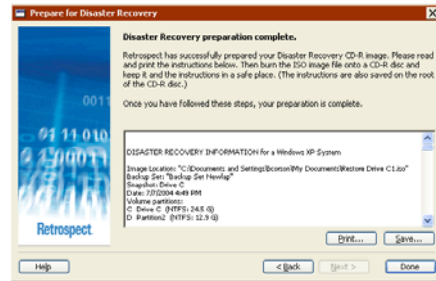
The scrollable region specifies the location of the ISO file and summarizes your Disaster Recovery instructions.

Click the Save button to specify a location to save them as a text file. (The same instructions are already in a text file on the CD image.) Click Print to print the instructions and keep them in a safe place with the Backup Set media, a copy of the Catalog File on CD, and the CD image. Click Done to leave the wizard.

At this point, you are done with Retrospect's Disaster Recovery preparation. You may now burn the image to CD or store the image for future use.

Keeping Preparations Up to Date

After you have prepared for Disaster Recovery, you can continue to back up to the Backup Set you used to prepare for Disaster Recovery. This ensures that you will be able to restore the most up-to-date information. There are three situations in which you should create a new Disaster Recovery CD or image:

• If you do a Recycle backup (page 25) to the Backup Set you used to prepare for Disaster Recovery.

• If you begin backing up the computer to a different Backup Set (other than the one selected in the preparation wizard). This includes New Backup Set backups (page 25), that use different Backup Sets.

• If you add new hardware to the computer or otherwise change its hardware configuration

(including interface cards, backup devices, and device drivers).

To update a computer's Disaster Recovery CD or image, use the wizard and select the Snapshot from the computer's most recent backup.

RESTORING THE BACKUP COMPUTER

There are three methods you can use to restore the Windows backup computer in the event of a disaster:

- Restoring from a Disaster Recovery CD
- Restoring from a Full Backup
- Restoring from a Partial Backup

Restoring from a Disaster Recovery CD

If disaster strikes, gather the Disaster Recovery CD and/or the printed instructions you created with the Disaster Recovery preparation wizard. The printed instructions specify the Backup Set required for Disaster Recovery. Gather all the media for this Backup Set. The instructions provide customized step-by-step procedures for accomplishing the two main goals of Disaster Recovery:

- Installing a temporary Windows OS
- Restoring the system volume using a Retrospect Snapshot

When you start the computer using the Retrospect Disaster Recovery CD, the Disaster Recovery process begins automatically and steps you through the recovery process.

Restoring from a Full Backup

If your computer has encountered a disastrous data loss that cannot be easily remedied, but you do not have a Disaster Recovery CD or customized instructions, you can still restore the backup computer from a full backup using the following procedure.

The steps below, which should be taken only in the event of serious trouble, involve completely replacing the contents of your hard drive with a previous backup in which you backed up "all files."

NOTE: To restore from a partial backup in which you backed up only some of the files, follow the instructions under "Restoring from a Partial Backup" on page 209.

1. Restart and Try to Repair the Disk

Find the CD-ROM included with your computer or the emergency recovery disk. Restart your computer, and put in the disk or CD. When your computer has started from this disk or CD, run ScanDisk to examine your hard disk for problems. (You should also try other disk repair utilities if you have them.)

2. Assess the Current State of the Hard Disk

If you were able to repair all damage and no low-level problems are found, stop here! You do not need to restore or reformat your hard disk.

If you could not make any repairs with the disk utilities, or if the hard disk still is not accessible from Windows Explorer, you probably need to reformat your hard disk. Go on to step 4.

If you were able to repair some damage, but problems remain with the hard disk, you may need to reformat it. But first you must safeguard your data as described in step 3.

3. Make New Backups Before Reformatting

Now is a good time to back up your repaired hard disk. You may want to make two new backups (with the Thorough verification option on) to new Backup Sets. (Do not do a Recycle backup to an existing Backup Set, as the damaged drive might not have all of your files on it and you don't want to erase your previous backups.) Once you are sure you have redundant backups of your data, copy your Backup Set

Catalogs to a floppy disk, removable disk, or server.

4. Reformat the Disk

If the disk repair utility cannot fix the disk, you may have to erase or reformat the disk in order to prepare it for restoration.

WARNING: Erasing or formatting a hard disk destroys all data stored on the disk. If you are not sure whether you should erase or format your hard disk, contact its vendor for assistance.

5. Re-install Software

Install new Windows operating system software on your newly-formatted hard disk. (For a Windows Me upgrade, use the Windows 98 CD.) Restart from this volume.

Make sure to install the same operating system version and service pack that was running when you backed up the computer. For example, if you are restoring from a backup of a computer that was running Windows XP with Service Pack 2, make sure to install Service Pack 2 on the newly-formatted disk.

NOTE: You may also need to install third-party drivers in order to access backup devices.

Install Retrospect. If you copied your Catalog Files to floppy or removable disks, copy them back to your hard disk.

Start the Retrospect application and enter your license code when prompted. If you did not make copies or backups of your Catalog Files, recreate the Catalog or Catalogs from your storage media. See "Recreating a Catalog" on page 302 for more information.

If you copied your Catalog Files from a CD/DVD or removable disk you must get Retrospect to recognize them. From the navigation bar, click Configure>Backup Sets, then click More and Open to add the Catalogs to the list of available Backup Sets.

6. Restore from Backup

Now that your hard disk is working again and Retrospect is available along with your backup Catalogs, you can restore your hard disk. Choose Restore>Restore from the Retrospect navigation bar. The Restore Wizard displays. Click Next to begin restoring.
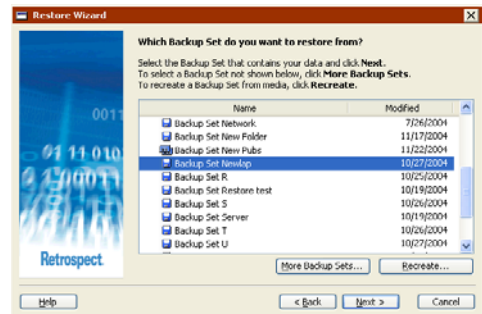
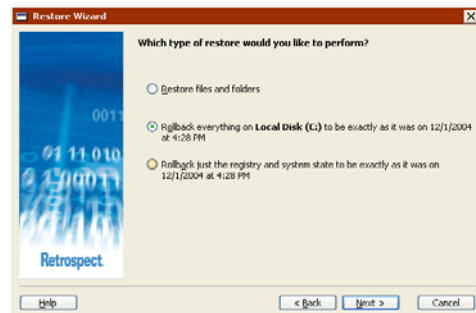Select the Backup Set that contains the full backup from which you want to restore, then click Next.
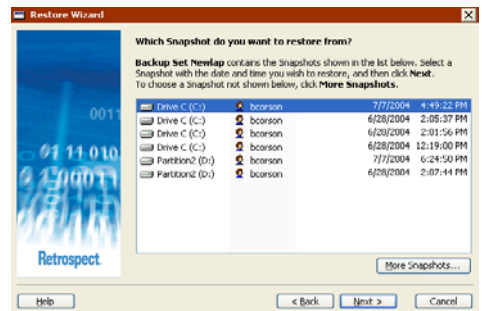
You can restore your computer to its exact state at any point in time for which a full system Snapshot exists. Select the Snapshot to restore, then click Next.

Choose "Original location" as the destination to which to restore files, then click Next. If the "Original location" option is not available, choose 'New location" and select your hard drive manually.
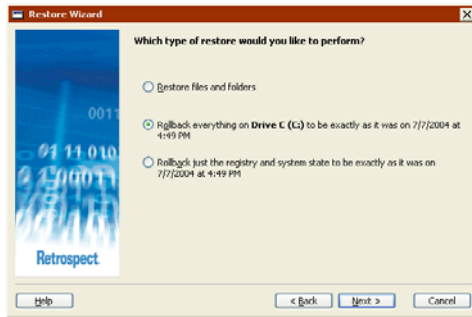
Because your whole hard disk was wiped out and needs to be completely restored, choose "Rollback everything...", then click Next. This option restores all the files in the Snapshot to the destination. This option also restores the registry and System State information from the source Snapshot.

Click Preview Files to view the files that will be restored, or click Next to display the Restore Wizard summary screen. Click Start in the summary screen to begin restoring.

7. Restart to Finish

After Retrospect finishes copying the files, exit Retrospect and restart the computer. The Retrospect Helper service runs automatically and finishes restoring the registry and System State. When it finishes, your computer is ready to use.

Restoring from a Partial Backup

If your computer has encountered a disastrous data loss that cannot be easily remedied, but you do not have a Disaster Recovery CD, customized instructions, or a even full backup, you can still restore the backup computer from a partial backup using the following procedure.

1. Get the Computer Working

Follow steps one through four of "Restoring from a Full Backup," which starts on page 207.

Install new Windows operating system software on your newly-formatted hard disk. Eject any

CDs and restart to boot from the new operating system on the hard disk.

2. Get Retrospect Working

Install Retrospect from the Retrospect CD. Start the Retrospect application and enter your license code when prompted.

If you copied your Catalog Files from a CD/DVD or removable disk you must get Retrospect to recognize them. From the navigation bar, click Configure>Backup Sets, then click More and Open to add the Catalogs to the list of available Backup Sets.

If you did not make copies or backups of your Catalog Files, recreate the Catalog or Catalogs from your storage media. See "Recreating a Catalog" on page 302 for more information.

3. Restore from Backup

Now that your hard disk is working again and Retrospect is available along with your backup Catalogs, you can restore your hard disk. Choose Restore>Restore from the Retrospect navigation bar. The Restore Wizard displays. Click Next to begin restoring.
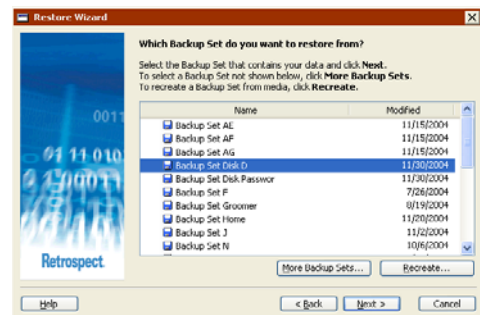
Select the Backup Set that contains the partial backup from which you want to restore, then click Next.
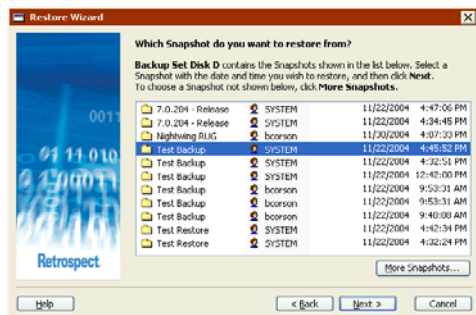
Select the Snapshot to restore, then click Next.

TIP: If you have Snapshots for multiple volumes, you'll need to repeat Step 3 for each volume to restore all the files and folders for which a backup exists.

Choose "Original location" as the destination to which to restore files, then click Next. If the "Original location" option is not available, choose 'New location" and select your hard drive manually.
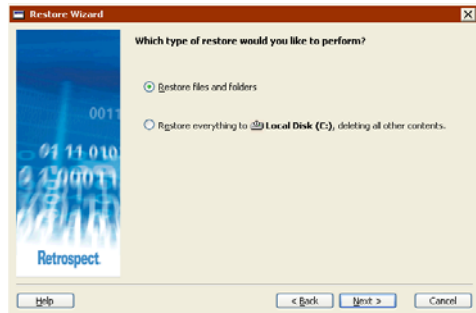
Because you are restoring from a partial backup, choose "Restore files and folders", then click Next. This option allows you to restore some or all of the files in the Snapshot, while leaving existing files on the destination as is. this is especially important when you are doing multiple partial restores to the same destination.

Click Select Files to view and select the files to restore. Click OK in the file selection window, then click Next.
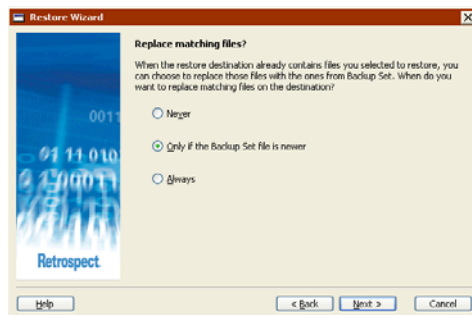
If you are doing multiple partial restores to the same destination, choose "Only if the Backup Set file is newer". That way if different versions of the same file are contained in different volume Snapshots, Retrospect will only replace the file on the destination if the file in the Snapshot is more recent.

Click Next to display the Restore Wizard summary screen. Click Start in the summary screen to begin restoring.

Repeat step 3 for each volume for which you have a Snapshot.

RESTORING CLIENT COMPUTERS

The process for restoring client computers is different than the process of restoring the back-up computer.

NOTE: You cannot restore clients set up for read access only.

This section describes:

- Restoring Clients from a Disaster Recovery CD
- Restoring a Windows Client
- Restoring a Mac OS Client
- Restoring Mac OS File Servers
- Restoring a UNIX Client
- Restoring a NetWare Client

Restoring Clients from a Disaster Recovery CD

Retrospect can create client disaster recovery CDs for Windows clients (except Windows 95 and Windows NT 4.0), provided that you have the required license. If you created a disaster recovery CD for a client, the restoring process is greatly simplified.

Find the disaster recovery CD and/or the printed instructions you created with the Disaster Recovery preparation wizard. The printed instructions specify the Backup Set required for Disaster Recovery. Gather all the media for this Backup Set. The instructions provide customized step-by-step procedures for accomplishing the three main goals of Disaster Recovery:

- Installing a temporary Windows OS
- Installing a temporary Retrospect Client
- Restoring the client system volume from the backup computer using a Retrospect Snapshot

When you start the client computer using the Retrospect Client Disaster Recovery CD, the Disaster Recovery process begins automatically and walks you through the first two steps of the recovery process. The disaster recovery instructions included on the CD describe how to restore the client from the backup computer.

Restoring a Windows Client

If you don't have a Retrospect Client Disaster Recovery CD or printed instructions, follow these steps:

1. Restart and Try to Repair the Disk

Find the CD-ROM included with your computer or the emergency recovery disk. Restart your computer, and put in the disk or CD. When your computer has started from this disk or CD, run ScanDisk to examine your hard disk for problems. (You should also try other disk repair utilities if you have them.)

2. Assess the Current State of the Hard Disk

If you were able to repair all damage and no low-level problems are found, stop here! You do not need to restore or reformat your hard disk.

If you could not make any repairs with the disk utilities, or if the hard disk still is not accessible from Windows Explorer, you probably need to reformat your hard disk. Go to step 4. Reformat the Disk.

If you were able to repair some damage, but problems remain with the hard disk, you may need to reformat it. But first you must safeguard your data as described below in step 3. Make New Backups Before Reformatting.

3. Make New Backups Before Reformatting

Now is a good time to back up your repaired hard disk. You may want to make two new backups (with the Thorough verification option on) to new Backup Sets. (Do not do a Recycle backup to an existing Backup Set, as the damaged drive might not have all of your files on it and you don't want to erase your previous backups.) Once you are sure you have redundant backups of your data, copy your Backup Set Catalogs to a CD/DVD, removable disk, or server.

4. Reformat the Disk

If the disk repair utility cannot fix the disk, you may have to erase or reformat the disk in order to prepare it for restoration.

WARNING: Erasing or formatting a hard disk destroys all data stored on the disk. If you are not sure whether you should erase or format your hard disk, contact its vendor for assistance.

5. Re-install Software

Install new Windows operating system software on your newly-formatted hard disk. Restart from this volume. (If you are going to restore a dual-boot system that includes NT or 2000, in-

stall NT or 2000 and do the following steps from NT or 2000.)

6. Configure TCP/IP

Make sure the computer is properly set up for use with TCP/IP networking. (If you need help configuring TCP/IP see your network administrator.)
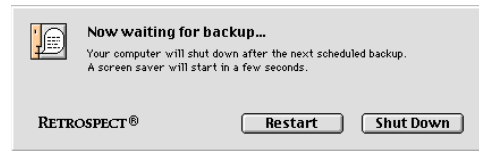
7. Install Client Software

Use the Setup program to install the client software as instructed in "Installing Retrospect Client Software on Windows Computers" on page 167.

8. Prepare Client Database

From the backup computer, forget the old client, then log in the new client.

9. Restore Files

Now that the hard disk is working again, you can restore the client over the network from the backup computer. Choose Restore>Restore from the Retrospect navigation bar. The Restore Wizard displays. Click Next to begin restoring.
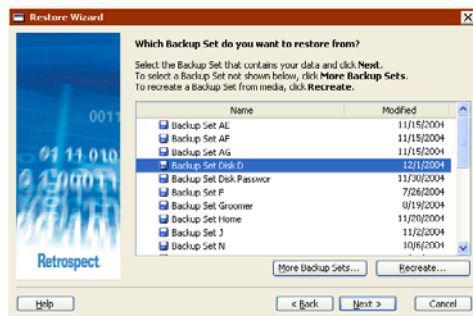
Select the Backup Set that contains a full backup of the Windows client computer, then click Next.

You can restore the client computer to its exact state at any point in time for which a full system Snapshot exists. Select the Snapshot to restore, then click Next.

Choose "Original location" as the destination to which to restore files, then click Next. If the "Original location" option is not available, choose "New location" and select the client computer's hard drive manually.

Because the client's entire hard disk was wiped out and needs to be completely restored, choose "Rollback everything...", then click Next. This option deletes all the existing files on the destination, then restores all the files in the Snapshot to the destination. This option also restores the client's registry and System State information from the source Snapshot.

Click Preview Files to view the files that will be restored, or click next to display the Restore Wizard summary screen. Click Start in the sum-

mary screen to begin restoring the client computer.

10. Clean Up

Restart the client computer. The Retrospect Helper service runs automatically and finishes restoring the registry and System State. When it finishes, your computer is ready to use.

Restoring a Mac OS Client

The following instructions tell how to restore an entire volume on a Mac OS client over the network.

You must first work at the client computer to get it operating with the network before performing the actual restore operation from the backup computer.

The steps below, which should be taken only in the event of serious trouble, involve completely replacing the contents of a client computer's hard drive with a previous backup in which you backed up "all files" or "all files except cache".

NOTE: The steps below are not for a Macintosh that serves data via file sharing or AppleShare. To restore a server, see "Restoring Mac OS File Servers" on page 215.

1. Restart and Try to Repair the Disk

Find the Mac OS 9 or Mac OS X CD-ROM, restart the Macintosh, and put in the CD. Press and hold the "C" key during startup to force the computer to boot from the CD-ROM. Under Mac OS 9, open the Disk First Aid utility application from the CD. Under Mac OS X, choose Open Disk Utility from the Installer menu then click the First Aid tab. Use Disk First Aid to examine the hard disk for problems and repair them, if possible. (You should also try other disk repair utilities if you have them.) Use the low-level verification or test function of the Drive Setup utility or your disk formatter to examine the hard disk for defects that other utilities will not find.

2. Assess the Current State of the Hard Disk

If you were able to repair all damage and no low-level problems are found, stop here! You do not need to restore or reformat your hard disk.

If you could not make any repairs with the disk utilities, or if the hard disk still does not mount on the Desktop, you probably need to reformat your hard disk. Go to step 4. Reformat the Disk.

If you were able to repair some damage, but problems remain with the hard disk, you may need to reformat it. But first you must safeguard your data as described below in step 3. Make New Backups Before Reformatting.

3. Make New Backups Before Reformatting

Now is a good time to back up the repaired hard disk. You may want to make two new backups (with the Thorough verification option on) to new Backup Sets. (Do not do a Recycle backup to an existing Backup Set, as the damaged drive might not have all of your files on it and you don't want to erase your previous backups.)

4. Reformat the Disk

If the disk repair utilities could not fix the disk, you may have to erase or reformat the disk in order to prepare it for restoration.

WARNING: Erasing or formatting a hard disk destroys all data stored on the disk. If you are not sure whether you should erase or format your hard disk, contact its vendor for assistance.

If the disk is beyond repair under Mac OS 9, use the Finder to select the damaged volume and choose Erase Disk from the Special menu. If the disk is beyond repair under Mac OS X, use Disk Utility to select the damaged volume, click the Erase tab, choose a format, supply a name, and click Erase. If erasing is unsuccessful from the Mac OS 9 Finder, you need to reformat the disk. To do this, start the Drive Setup application from the Disk Tools disk or CD, or the

formatting software that came with the hard disk, and use it to format the hard disk.

5. Install System Software

Install new Mac OS system software on the newly-formatted hard disk. Restart the Macintosh from the Mac OS 9 or Mac OS X CD-ROM, pressing and holding the "C" key during startup to force the computer to boot from the CD.
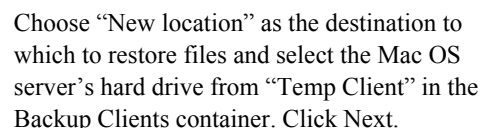
Install new Mac OS system software on the newly-formatted hard disk. You must install the same exact version number of Mac OS X as the version of Mac OS X you will restore. For example, if the client was backed up running version 10.2.4, you must install Mac OS X 10.2.4.

Eject any CDs and restart from the new system on the hard disk. Use the Date & Time control panel or system preference to set your local time and time zone, and, if necessary, change the Daylight Saving setting. Under Mac OS 9, rename the System Folder to "temp."

6. Configure TCP/IP

Make sure the computer is properly set up for use with TCP/IP networking. (If you need help configuring TCP/IP see your network administrator.)

7. Install Client Software

Install Retrospect client software on the Macintosh and restart it. From the backup computer, forget the old client, then log in this new client.

8. Prepare the Client Macintosh for Restore

Open the Retrospect client control panel (under Mac OS 9) or Retrospect Client application (Mac OS X) and verify the client software is turned on and is waiting for first access.

For ideal restoring conditions under Mac OS 9, shut down the client Macintosh so the Retrospect client shutdown dialog appears.

Leave the client Macintosh with this dialog; do not shut down or restart.

Before restoring to a volume other than the current system volume under Mac OS X, use the Finder's Show Info command on the volume. Choose Privileges from the info window's menu then turn off the "Ignore privileges on this volume" option.

For ideal restoring conditions under Mac OS X, log out so the single-user login window or multiple-user login list window appears. Leave the client Macintosh at this window; do not log in, shut down, or restart.

9. Restore Files

Now that the hard disk is working again, you can restore the client over the network from the backup computer. Choose Restore>Restore from the Retrospect navigation bar. The Restore Wizard displays. Click Next to begin restoring.

Select the Backup Set that contains a full backup of the Mac OS client computer, then click Next.
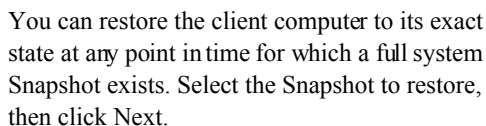
You can restore the client computer to its exact state at any point in time for which a full system Snapshot exists. Select the Snapshot to restore, then click Next.

Choose "Original location" as the destination to which to restore files, then click Next. If the "Original location" option is not available, choose "New location" and select the client computer's hard drive manually.

Because the client's entire hard disk was wiped out and needs to be completely restored, choose "Restore everything...", then click Next. This option deletes all the existing files on the destination, then restores all the files in the Snapshot to the destination.

Click Preview Files to view the files that will be restored, or click next to display the Restore Wizard summary screen. Click Start in the summary screen to begin restoring the client computer.

10. Restart, Rebuild, and Discard
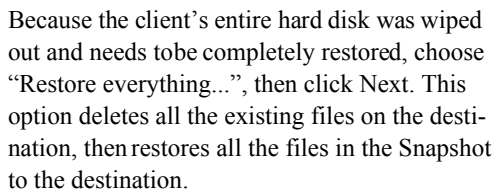
When the restore is completed, for Mac OS X clients, restart the computer. For Mac OS 9 clients, restart the computer and rebuild its desktop by pressing and holding both the Command and Option keys while the Macintosh starts (until the Macintosh asks you to confirm rebuilding the desktop). After it starts and rebuilds the desktop, place the "temp" System Folder in the Trash and empty the Trash.

Your computer is now ready to use.

TIP: If you often restore clients consider setting up a hard disk with System software and a logged in Retrospect Client control panel. Connect this hard disk to the Macintosh you need to restore and you are well on your way to restoring more quickly. Just boot off this drive to restore all your clients without having to reinstall the operating system.

Restoring Mac OS File Servers

This section describes how to use Retrospect to restore volumes shared by Mac OS file sharing. These operations require special procedures to ensure access privileges are intact after the volume is restored.

Access privileges are restored for a server only if file sharing was active when the backup was made *and* if file sharing is active during the restore operation.

If your server is undamaged and you need to restore only some of the files and folders from a backup (for instance, because somebody accidentally deleted some folders from the server), just follow one of the sets of instructions in "Restore" on page 69.

If you need to restore an entire server, use the following procedure.

1. Restart and Try to Repair the Disk

Find your Mac OS 9 or Mac OS X CD-ROM, restart your Macintosh, and put in the CD. Press

and hold the "C" key during startup to force the computer to boot from the CD-ROM. Under Mac OS 9, open the Disk First Aid utility application from the CD. Under Mac OS X, choose Open Disk Utility from the Installer menu then click the First Aid tab. Use Disk First Aid to examine your hard disk for problems and repair them, if possible. (You should also try other disk repair utilities if you have them.) Use the low-level verification or test function of the Drive Setup utility or your disk formatter to examine the hard disk for defects that other utilities will not find.

2. Assess the Current State of the Hard Disk

If you were able to repair all damage and no low-level problems are found, stop here! You do not need to restore or reformat your hard disk.

If you could not make any repairs with the disk utilities, or if the hard disk still does not mount on the Desktop, you probably need to reformat your hard disk. Go on to step 4.

If you were able to repair some damage, but problems remain with the hard disk, you may need to reformat it. But first you must safeguard your data as described below in step 3.

3. Make New Backups Before Reformatting

Now is a good time to back up your repaired hard disk. You may want to make two new backups (with the Thorough verification option on) to new Backup Sets. (Do not do a Recycle backup to an existing Backup Set, as the damaged drive might not have all of your files on it and you don't want to erase your previous backups.) Once you are sure you have redundant backups of your data, copy your Backup Set Catalogs to a floppy disk, removable disk, or another server.

4. Reformat the Disk

If the disk repair utility cannot fix the disk, you may have to erase or reformat the disk in order to prepare it for restoration.

WARNING: Erasing or formatting a hard disk destroys all data stored on the disk. If you are not sure whether you should erase or format your hard disk, contact its vendor for assistance.

If the disk is beyond repair under Mac OS 9, use the Finder to select the damaged volume and choose Erase Disk from the Special menu. If the disk is beyond repair under Mac OS X, use Disk Utility to select the damaged volume, click the Erase tab, choose a format, supply a name, and click Erase. If erasing is unsuccessful from the Mac OS 9 Finder, you need to reformat the disk. To do this, start the Drive Setup application from the Disk Tools disk or CD, or the formatting software that came with the hard disk, and use it to format your hard disk.

5. Install System Software

Restart the Macintosh from the Mac OS 9 or Mac OS X CD-ROM, pressing and holding the "C" key during startup to force the computer to boot from the CD.

Install new Mac OS system software on the newly-formatted hard disk. You must install the same exact version number of Mac OS X as the version of Mac OS X you will restore. For example, if the client was backed up running version 10.2.4, you must install Mac OS X 10.2.4.

Eject any CDs and restart from the new system on the hard disk. Use the Date & Time control panel or system preference to set your local time and time zone, and, if necessary, change the Daylight Saving setting. Under Mac OS 9, rename the System Folder to "temp."

6. Configure TCP/IP

Make sure the computer is properly set up for use with TCP/IP networking. (If you need help

configuring TCP/IP see your network administrator.)

7. Install Client Software

Install Retrospect client software on the Macintosh and restart it. Log this client into Retrospect and name it Temp Client.

8. Prepare the Client Macintosh for Restore

Open the Retrospect client control panel (under Mac OS 9) or Retrospect client application (Mac OS X) and verify the client software is turned on and is waiting for first access.

For ideal restoring conditions under Mac OS 9, shut down the client Macintosh so the Retrospect client shutdown dialog appears.

Leave the client Macintosh with this dialog; do not shut down or restart.

Before restoring to a volume other than the current system volume under Mac OS X, use the Finder's Show Info command on the volume. Choose Privileges from the info window's menu then turn off the "Ignore privileges on this volume" option.

For ideal restoring conditions under Mac OS X, log out so the single-user login window or multiple-user login list window appears. Leave the client Macintosh at this window; do not log in, shut down, or restart.

9. Restore Files

Now that the hard disk is working again, you can restore the server over the network from the backup computer. Choose Restore>Restore from the Retrospect navigation bar. The Restore Wizard displays. Click Next to begin restoring.

Select the Backup Set that contains a full backup of the Mac OS server client computer, then click Next.

You can restore the Mac OS server to its exact state at any point in time for which a full system Snapshot exists. Select the Snapshot to restore, then click Next.

Choose "New location" as the destination to which to restore files and select the Mac OS server's hard drive from "Temp Client" in the Backup Clients container. Click Next.

WARNING: Before restoring to a volume other than the current system volume under Mac OS X, use the Finder's Show Info command on the volume. Choose Privileges from the info window's menu then turn off the "Ignore privileges on this volume" option.
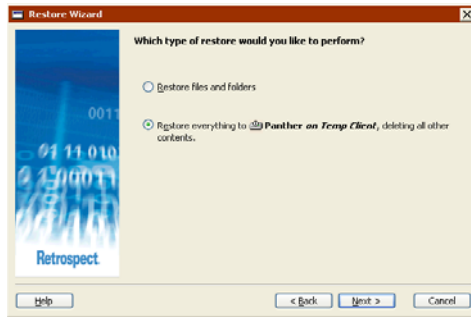
Because the Mac OS server's entire hard disk was wiped out and needs to be completely restored, choose "Restore everything...", then click Next. This option deletes all the existing files on the destination, then restores all the files in the Snapshot to the destination.

Click Preview Files to view the files that will be restored, or click next to display the Restore Wizard summary screen. Click Start in the summary screen to begin restoring the client computer.

When Retrospect is finished restoring, restart the Mac OS server client computer. Discard the "temp" System Folder by placing it in the Finder's Trash can and emptying the Trash. Then, use Retrospect to forget the Temp Client and log in the original client.

10. Extra Steps for Mac OS 9
If you are using Mac OS file sharing, start file sharing. Choose the volumes or folders you wish to share, then select the appropriate Owner and Group for root access privileges and set your desired options.

With sharing on, perform another restore operation using the same Snapshot and the "restore

everything..." method. Retrospect performs a "smart" incremental restore, copying only a few files (or none if no files have changed), and then sets the access privileges. Retrospect may report sharing violation errors but they are not significant and you should ignore them.

Restart the server, and rebuild the Desktop by holding down the Command and Option keys until a confirming dialog appears.

NOTE: This step is only required for Mac OS 9 servers.

11. Extra steps for Mac OS X.1.x
After restarting the computer, share points may be missing or replaced with improper share points. Using Server Admin, take the following steps to correct these problems:

• Remove invalid share points.
• Re-establish desired share points.
• Reset the Home Directory Defaults for any affected users and groups lists (or NetInfo domains).

NOTE: These extra steps are not required for Mac OS X Server 10.2 and later.

Restoring a UNIX Client
If the UNIX client computer is undamaged and you need to restore only some of the files and folders from a backup, just follow one of the sets of instructions in "Restore" on page 69.

If the UNIX client computer crashes or suffers from other serious problems, you must take the following approach.

1. Restart and Try to Repair the Disk
If you have a boot disk for your system, restart the client computer, and put in the disk. When the computer has started from this disk, follow the instructions to repair your disk.

Alternatively, you can boot the system and run a file system check (fsck or equivalent). If this

does not result in a bootable system, you have two options, depending on your expertise with the operating system. For the experienced administrator, boot to single-user mode from your OS installation media and repair the boot sector, replace the kernal, etc. If you have less experience, or do not feel comfortable with the above steps, you should re-install the OS, after replacing the hard disk (if necessary).

2. Assess the Current State of the Hard Disk

If you were able to repair all damage and no low-level problems are found, stop here! You do not need to restore or reformat the hard disk.

If you could not make any repairs with the boot disk, or if the hard disk still is not accessible, you probably need to reformat the hard disk. Go to step 4. Reformat the Disk.

If you were able to repair some damage, but problems remain with the hard disk, you may need to reformat it. But first you must safeguard your data as described below in step 3. Make New Backups Before Reformatting.

3. Make New Backups Before Reformatting

Now is a good time to back up the repaired hard disk. You may want to make two new backups (with the Thorough verification option on) to new Backup Sets. (Do not do a Recycle backup to an existing Backup Set, since the damaged drive might not have all files on it and you do not want to erase previous backups.) Once you are sure you have redundant backups of your data, copy your Backup Set Catalogs to a removable disk or server.

4. Reformat the Disk

If the boot disk cannot fix the hard disk, you may have to erase or reformat the hard disk in order to prepare it for restoration.

WARNING: Erasing or formatting a hard disk destroys all data stored on the disk. If you are not sure whether you should erase or format your hard disk, contact its vendor for assistance.

5. Re-install Software

Install new UNIX operating system software on the newly-formatted hard disk, making sure to create the same mount points as the original system. Restart from this volume.

6. Install Client Software

Use the Setup program to install the client software as described in "Installing the Client Software on UNIX Computers" on page 169.

7. Prepare Client Database

From the backup computer, forget the old client, then log in the new client.

8. Restore Files

Now that the hard disk is working again, you can restore the client over the network from the backup computer. Choose Restore>Restore from the Retrospect navigation bar. The Restore Wizard displays. Click Next to begin restoring.
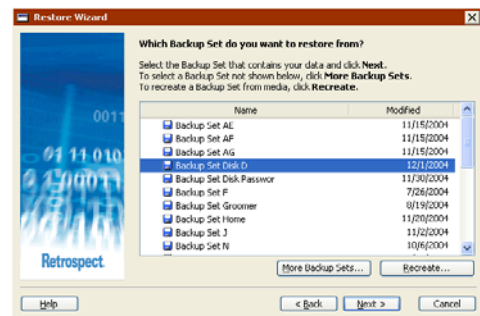
Select the Backup Set that contains a full backup of the UNIX client computer, then click Next.

You can restore the client computer to its exact state at any point in time for which a full system Snapshot exists. Select the Snapshot to restore, then click Next.

Choose "Original location" as the destination to which to restore files, then click Next. If the "Original location" option is not available, choose the client computer's hard drive manually.

Because the client's entire hard disk was wiped out and needs to be completely restored, choose "Restore everything...", then click Next. This option deletes all the existing files on the destination, then restores all the files in the Snapshot to the destination. This option also restores the client's registry and System State information from the source Snapshot.

Click Preview Files to view the files that will be restored, or click next to display the Restore Wizard summary screen. Click Start in the summary screen to begin restoring the client computer.

9. Clean Up
Restart the client computer.

Restoring a NetWare Client
If the NetWare client computer is undamaged and you need to restore only some of the files and folders from a backup, just follow one of the sets of instructions in "Restore" on page 69.

If the NetWare client computer crashes or suffers from other serious problems, you must take the following approach.

1. Restart and Try to Repair the Disk
Restart the client computer using a bootable NetWare CD. When the computer has started from this disk, attempt to repair your disk using available utilities.

If cannot repair the disk to make it bootable, you should re-install the OS, after replacing the hard disk (if necessary). Go to step 5. Re-install NetWare.

2. Assess the Current State of the Hard Disk
If you were able to repair all damage and no low-level problems are found, stop here! You do not need to restore or reformat the hard disk.

If you could not make any repairs from the boot disk, or if the hard disk still is not accessible, you probably need to reformat the hard disk. Go to step 4. Reformat or Replace the Disk.

If you were able to repair some damage, but problems remain with the hard disk, you may need to reformat it. But first you must safeguard your data as described below in step 3. Make New Backups Before Reformatting.

3. Make New Backups Before Reformatting
Now is a good time to back up the repaired hard disk. You may want to make two new backups (with verification on) to new Backup Sets. (Do not do a Recycle backup to an existing Backup Set, since the damaged drive might not have all files on it and you do not want to erase previous backups.) Once you are sure you have redundant backups of your data, copy your Backup Set Catalogs to a removable disk or server.

4. Reformat or Replace the Disk
If you cannot repair the hard disk, you may have to erase or reformat it in order to prepare it for restoration.

WARNING: Erasing or formatting a hard disk destroys all data stored on the disk. If you are not sure whether you should erase or format your hard disk, contact its vendor for assistance.

If all else fails you may have to replace the hard disk.

5. Re-install NetWare

Install the NetWare operating system on the newly-formatted (or new) hard disk. Make sure it is the same version of NetWare and the same service pack as the NetWare server you backed up. Restart from this volume.

6. Install Client Software

Install the client software as described in "Installing Retrospect Client Software on NetWare Computers" on page 170.

7. Prepare Client Database

From the backup computer, forget the old client, then log in the new client.

8. Restore eDirectory and Files

Now that the hard disk is working again, you can restore the client over the network from the backup computer. Choose Restore>Restore from the Retrospect navigation bar. The Restore Wizard displays. Click Next to begin restoring.

Select the Backup Set that contains a full backup of the NetWare client computer, then click Next.

You can restore the client computer to its exact state at any point in time for which a full system Snapshot exists. Select the Snapshot to restore, then click Next.

NOTE: You must restore eDirectory first, before restoring the rest of your data.

Choose "Original location" as the destination to which to restore files, then click Next. If the "Original location" option is not available, choose the client computer's hard drive manually.

Because the client's entire hard disk was wiped out and needs to be completely restored, choose "Restore everything...", then click Next. This option deletes all the existing files on the destination, then restores all the files in the Snapshot to the destination.

Click Preview Files to view the files that will be restored, or click next to display the Restore Wizard summary screen. Click Start in the summary screen to begin restoring the client computer.

9. Clean Up

Restart the client computer.

MANAGEMENT

- **BACKUP STRATEGIES**

- **LOG AND REPORTS**

- **REPORTSWATCHER**

- **EXECUTION OPTIONS**

- **MANAGING BACKUP SETS**

- **MAINTAINING SCRIPTS**

- **RETROSPECT PREFERENCES**

- **MOVING RETROSPECT**

- **CATALOG AND CONFIGURATION BACKUPS**

- **WORKING WITH FILE SERVERS**

- **WORKING WITH OPEN FILES**

- **TERMINAL SERVICES AND REMOTE DESKTOP**

This chapter describes how to perform various tasks to manage Backup Sets and scripts, including viewing reports, and maintaining scripts. It offers several strategies for doing backups. It also offers advice on using Retrospect and describes techniques for more effective backups, including tips on Open File Backup and using Retrospect with other software.

BACKUP STRATEGIES

This section suggests several strategies for backing up your computer or your entire network. Review each strategy and decide which will work best for your situation. Perhaps you will need to slightly modify a strategy to better fit your needs. Perhaps you will devise your own strategy which bears no relation to these suggestions. Realize these are but a few suggested strategies, and Retrospect's features allow an unlimited number of different strategies. Just remember the basic backup rules when you go about creating a backup strategy of your own.

The different backup actions available with Retrospect are integral to developing successful strategies. They are described in "Backup Actions" on page 24.

Basic Backup Rules

While Retrospect is a powerful tool for safeguarding your data, it is most effective when you follow some basic backup rules:

- Back up often because you cannot restore what is not backed up. For example, if your hard disk malfunctions today but you most recently backed it up a week ago, you have lost the data you have accumulated over the week. Retrospect is most effective when you back up everything and back up often, which you can ensure by setting up scripts to automate backups.

- Keep multiple backups of your data. Rotate among different Backup Sets. Using more Backup Sets makes you less likely to lose data if you misplace or damage media.

- Retire old media on a regular schedule. Regularly introduce new media using New Backup Set backups, because having all of your backups on one media set leaves you too vulnerable. (If even one tape of a set is damaged, you no longer have a complete backup.) A benefit of new media in your

backup strategy is that it is faster to restore from a few media members than to restore from a set that has many members and backup sessions.

- Use meaningful names for your Backup Sets based on what they contain and how often they get rotated and then label your media appropriately.

- Always store at least one Backup Set off-site to guard against fire, theft, and natural disaster.

- Back up the backup computer. You probably have put more time and energy than you realize into your Retrospect configuration and catalogs.

- Take care of your backup media, which can easily be damaged by the environment. Media can also wear out after as few as several hundred uses. See "Media Longevity and Storage" on page 50 for more information.

- Make sure to verify your backups, either during backup using the Thorough or Media verification options, or after a backup has finished using a verification script or the Verify Media command.

- Back up your Catalog Files to their own Backup Set. See "Catalog Backups" on page 273.

Individual Backup Strategies

The following strategies are useful for backing up a single computer. If you need to back up more than one computer, see "Network Backup Strategies".

Individual Strategy 1- Run Documents

Create an unscheduled backup script and save it as a run document. See "Manual Script Execution," which starts on page 139. Set the backup action to Normal. Make a second run document from the same script, but this time set the backup action to Recycle.

Execute the Normal backup run document daily or whenever you please, and every few weeks execute the Recycle backup run document to keep your Backup Sets from becoming large and cumbersome.

To introduce new media for rotation with other sets or off-site storage, periodically configure the Backup Set to use a new Backup Set, as described in "The Options tab" on page 256.

Individual Strategy 2- Scheduled Script

Create a backup script and schedule it to run automatically. Add a day of week schedule doing a Recycle backup every Friday and another doing Normal backups Monday through Thursday.

The two schedulers look like this:

Day of week schedulers

Recycle backup to 💾 Daily Backup
Every Friday, starting 12/3/2004 at 10:00 PM

Normal backup to 💾 Daily Backup
Every Mon/Tue/Wed/Thu, starting 12/6/2004 at 10:00 PM

To introduce new media for rotation with other sets or off-site storage, periodically configure the Backup Set to use a new Backup Set, as described in "The Options tab" on page 256.

Network Backup Strategies

When you need to back up a network of client computers, you must decide which kind of backup scripts to use. The table below lists situations which are suited to Proactive Backup scripts or regular backup scripts.

Situations Suiting Proactive Backup	Situations Suiting Backup Scripts
You have a backup computer dedicated solely to that purpose.	Your backup computer has other duties at other times.
You have too many clients with too much data to be entirely backed up in a single night.	Your scheduled backups are completed before the client computers are used in the mornings.
You find yourself trying to catch up with your backups, making special scripts and immediate backups for certain clients that are not completely backed up by your regular backup script.	Your scheduled backups are completed before the client computers are used in the mornings and unsuccessful backups are rare.
You have mobile clients and portable drive volumes that appear on the network at random times.	Your network includes only desktop computers, no removable disks or notebook computers.
You want Retrospect to back up to whatever media is in the backup device.	You always insert the correct media beforehand for unattended backups.

If you choose to use a strategy that includes Proactive Backup, skip ahead to "Network Strategy 4- Basic Proactive Backup" on page 227.

Network Strategy 1- Scheduled Script

Create a backup script. Set the destination to use three Backup Sets. Add a day of week scheduler to run the script daily to a particular Backup Set, every three weeks. Add a similar scheduler to run the script daily to the second Backup Set, every three weeks starting one week after the first scheduler. Add a similar scheduler to run the script daily to the third Backup Set, every three weeks starting one week after the second scheduler.

The three schedulers look like this:

Day of week schedulers

Normal backup to 📇 Red
     Every 3 weeks on .MTWTF., starting 9/10/2001 at 10:00 PM

Normal backup to 📇 Green
     Every 3 weeks on .MTWTF., starting 9/17/2001 at 10:00 PM

Normal backup to 📇 Blue
     Every 3 weeks on .MTWTF., starting 9/24/2001 at 10:00 PM

This strategy does not include scheduled Recycle and New Backup Set backup actions, so you should manually configure the Backup Sets for Recycle and New Backup Set backups at appropriate times. See "The Options tab" on page 256.

Network Strategy 2- Scheduled Script with Recycle and New Media Rotation

Create a backup script. Change the script destination to use three Backup Sets. Add a day of week scheduler to run a Normal backup Monday through Thursday to the first Backup Set, every three weeks. Add a day of week scheduler to do a Recycle backup to the first Backup Set on Friday, every three weeks. Add similar schedulers for the second and third Backup Sets, but set their starting dates one and two weeks later, respectively. Finally, add a repeating interval scheduler to do a New Backup Set backup to one of the Backup Sets every six weeks. (After a New Backup Set backup take

the old Backup Set media off site for safe keeping.)

The schedulers look like this:

Day of week scheduler
Day of week (or repeating interval) scheduler

Normal backup to 📇 Red
     Every 3 weeks on Mon/Tue/Wed/Thu, starting 9/10/2001 at 9:00 PM

Recycle backup to 📇 Red
     Every 3 weeks on Friday, starting 9/14/2001 at 7:00 PM

Normal backup to 📇 Green
     Every 3 weeks on Mon/Tue/Wed/Thu, starting 9/17/2001 at 9:00 PM

Recycle backup to 📇 Green
     Every 3 weeks on Friday, starting 9/21/2001 at 7:00 PM

Normal backup to 📇 Blue
     Every 3 weeks on Mon/Tue/Wed/Thu, starting 9/24/2001 at 9:00 PM

Recycle backup to 📇 Blue
     Every 3 weeks on Friday, starting 9/28/2001 at 7:00 PM

New Media backup to 📇 Red
     Every 6 weeks on Friday, starting 10/5/2001 at 7:00 PM

Repeating interval scheduler

Network Strategy 3- Scheduled Script with Rotating Daily Backup Sets

Make a script with five Backup Set destinations, named Monday through Friday. Add five day of week schedulers to back up to each respective Backup Set. Add five repeating interval schedulers to stagger Recycle backups every four weeks to each respective Backup Set, starting with Monday the first week, Tuesday the second week, and so on. But for Friday, make the repeating interval the last Friday of the month, doing a New Backup Set backup to the Friday Backup Set. (Take the old Backup Set media off site for safe keeping.)

The schedulers look like this:

Day of week scheduler

Normal backup to 🖳 <u>Monday</u>
Every Monday, starting 9/10/2001 at 10:00 PM
Normal backup to 🖳 <u>Tuesday</u>
Every Tuesday, starting 9/11/2001 at 10:00 PM
Normal backup to 🖳 <u>Wednesday</u>
Every Wednesday, starting 9/12/2001 at 10:00 PM
Normal backup to 🖳 <u>Thursday</u>
Every Thursday, starting 9/13/2001 at 10:00 PM
Normal backup to 🖳 <u>Friday</u>
Every Friday, starting 9/14/2001 at 10:00 PM
Recycle backup to 🖳 <u>Monday</u>
Every 4 weeks on Monday, starting 10/8/2001 at 7:00 PM
Recycle backup to 🖳 <u>Tuesday</u>
Every 4 weeks on Tuesday, starting 10/16/2001 at 7:00 PM
Recycle backup to 🖳 <u>Wednesday</u>
Every 4 weeks on Wednesday, starting 10/24/2001 at 7:00 PM
Recycle backup to 🖳 <u>Thursday</u>
Every 4 weeks on Thursday, starting 11/8/2001 at 7:00 PM
New Media backup to 🖳 <u>Friday</u>
Every month on the last Friday, starting 11/30/2001 at 7:00 PM

Repeating interval scheduler

NOTE: When you schedule the New Backup Set backup, make sure it occurs at the same time as the scheduled Friday Normal backups. When Retrospect encounters the New Backup Set backup scheduled for the same execution time as the Normal backup, it executes only the New Backup Set backup. If you were to schedule them at different times, both backups would execute.

Network Strategy 4- Basic Proactive Backup

Create a Proactive Backup script backing up all client sources. Schedule it to work from 7:00 P.M. to 7:00 A.M. during the work week (so as not to interfere with the users during their workdays) and all the time during weekends. Set the backup interval so Retrospect backs up every twelve hours.

Network Strategy 5- Basic Proactive Backup Including Mobile Computers

Duplicate the basic Proactive Backup script described above. Make mobile clients its only sources. Remove these volumes from the original script. Schedule the new script to run

twenty-four hours per day, with a backup interval of eighteen hours.

TIP: If you implement a strategy that includes Proactive Backup, read "Proactive Backup Tips and Techniques" on page 143. It includes information to help you devise a more effective strategy.

Network Strategy 6- On-Demand Proactive Backup

Create a Proactive Backup script backing up all client sources. Leave the schedule always active so it works twenty-four hours a day. Set the backup interval option so Retrospect backs up every ninety-nine days. Leave on the script option to allow early backup. Except for the initial backups when this strategy is first implemented, and every ninety-nine days thereafter, clients are not backed up unless they request it from their control panels. This strategy requires that you clearly communicate the responsibility to the users and, ideally, is supplemented with a regular backup script.

Staged Backup Strategies

Retrospect is designed to support staged backup with either an individual computer or a network of computers. Staged backup involves backing up to disk, then transferring the backups to tape. This takes advantage of the benefits of both disk and tape.

Disks are great at absorbing data transfers that arrive in bursts from network computers, resulting in faster backups than if you backed up directly to tape. Once data is backed up to disk, it can be easily transferred to tapes. The transfer from disk to tape is efficient because data from the disk arrives at a constant rate (no network bottlenecks), keeping your tape drive streaming forward at maximum speed. Tapes can then be stored offsite for safety, while disk backups stored onsite can be used to perform restores quickly.

Retrospect has many features that are useful for creating a staged backup strategy. Some ways to combine these features are discussed here, but there are countless possibilities for creating your own staged backup strategy using the following features:

- "Disk Grooming" on page 38
- "Scripted Backup Set Transfer" on page 124
- "Scripted Snapshot Transfer" on page 127
- "Backup Actions" on page 24
- "Disk Backup Sets and Multiple Executions" on page 161

TIP: The Tqzkq Retrospect web site includes a white paper that provides much more detailed information about implementing a disk-to-disk-to-tape staged backup strategy.

Staged Backup Strategy 1- Grooming and Backup Set Transfer

Start by creating a Proactive Backup script backing up all client sources. Schedule it to work from 7:00 P.M. to 7:00 A.M. during the work week and all the time during weekends. Set the backup interval so Retrospect backs up every twelve hours.

Use a disk Backup Set with grooming enabled as the destination. Set the grooming option so that Retrospect keeps at least the last 10 backups for each source. This ensures that you will have a 10 day rolling window of client data for quick local restores.

NOTE: The grooming policy you specify depends on how much data you are backing up and how big the destination disk is.

Create a Transfer Backup Sets script to transfer the disk Backup Set data to a tape Backup Set once a week. These tapes can be stored offsite for safety and can be used to restore older data that is eventually groomed from the disk Backup Set.

Transferring the Backup Set to tape provides a complete, redundant copy of the disk Backup Set. This includes all the Snapshots in the disk Backup Set and enables you to restore clients computers to any point in time for which a Snapshot exists.

Staged Backup Strategy 2- Grooming and Snapshot Transfer

Start by creating a Proactive Backup script backing up all client sources. Schedule it to work from 7:00 P.M. to 7:00 A.M. during the work week and all the time during weekends. Set the backup interval so Retrospect backs up every twelve hours.

Use a disk Backup Set with grooming enabled as the destination. Set the grooming option so that Retrospect keeps at least the last 10 backups for each source. This ensures that you will have a 10 day rolling window of client data for quick local restores.

NOTE: The grooming policy you specify depends on how much data you are backing up and how big the destination disk is.

Create a Transfer Snapshots script to transfer the disk Backup Set data to a tape Backup Set once a week. In the source Snapshots window, choose to transfer "The most recent Snapshot for each source" The first transfer results in what is called a "synthetic full" backup. A synthetic full backup includes the same files that a full backup done at the same time would, but it takes a lot less time and no network bandwidth. Each successive transfer copies only the Snapshots and files that don't already exist in the destination.

These tapes can be stored offsite for safety and can be used to restore older data that is eventually groomed from the disk Backup Set.

Transferring the most current Snapshots to tape provides a full backup of the client sources as they existed at the end of each week (when the

transfer script runs). This *does not* include additional Snapshots in the disk Backup Set from other points in time during the week (although these continue to exist in the disk Backup Set until it is groomed).

LOG AND REPORTS

Retrospect's reporting abilities lets you monitor execution history and error messages by viewing logs and reports. You may need to examine these to find out why an operation was unsuccessful in order to diagnose problems. Click Reports from Retrospect's navigation bar to access the logs and reports overview window.

NOTE: You can set Retrospect to provide e-mail notifications when it encounters errors, requires media, etc. See "E-mail Preferences" on page 271 for more information.

• The Backup Report shows a detailed account of backup operations for each local and networked volume.

• The Operations Log shows a record of each Retrospect operation, transaction, and event, and any errors that occurred.

• Session Contents shows the files that were actually backed up in a specific backup session.

• Database Backup History lists all database backups and includes information on the backup type and Backup Set. See Appendix A: SQL Server Agent and Appendix B: Exchange Server Agent for more information.

Viewing the Backup Report

Click Reports>Backup Report to view the Backup Report. An example of a Backup Report is shown below.

Unlike the Operations Log, to which Retrospect repeatedly appends new information, the Backup Report is completely updated each time a backup is performed. It allows you, as the backup administrator, to see, on a volume-by-volume basis, any problems with recent backups.

Understanding the Backup Report

The Backup Report can be viewed in two formats: Standard Format and Performance Data Format. See "Customizing the Backup Report"

Lack of report events indicates the volume has never been backed up

No errors means the backup was a complete success

a red ">" indicates the volume was not successfully backed up

on page 230 for information on how to switch between formats.

Both formats include the following information:

User/Volume is the source volume name. Client computer names, if logged in, are also listed. The date and time listed below a volume are the date and time of the most recent backup of the volume.

Script is the name of the script that did the most recent successful backup.

You can select a line in the report and open the script it refers to by using the Edit Script button. You can select a line in the report and click the Find in Log button to cross-reference the Operations Log. You can select any line listed in the report and clear it by choosing Clear from the Edit menu or by pressing the Delete key. If you clear a script or forget a Backup Set, that information is removed from the report. This may cause a volume to appear as if it was never backed up.

A *Standard Format* Backup Report contains the following information, in addition to User/Volume and Script:

Elapsed Days is the number of days since the backup.

Errors and Warnings indicates any errors or warnings that occurred for each backup. (Use the Find in Log command to isolate an error or warning in the Operations Log.)

Backup Set is the name of the Backup Set used for the most recent successful backup.

A *Performance Data Format* Backup Report contains the following information, in addition to User/Volume and Script:

Duration shows the time duration of the backup, in hours and minutes. Large numbers may indicate sources with heavy backup needs.

MB is the amount of data, in megabytes, backed up from the volume.

MB/Min is the speed, measured in megabytes per minute, of the source's backup. Abnormally slow performance may indicate problems with the network, backup device, or other hardware.

NOTE: Retrospect lets you specify an Execution performance threshold, which is useful for abandoning client backups that are too slow. See "Client Execution Options" on page 241

Customizing the Backup Report

You can use Report Options to display the Backup Report in Standard Format or Performance Data Format, specify the event types or event dates to include in the report, and various other options. Click the Report Options icon from the Backup Report toolbar to bring up a dialog in which you can make changes.
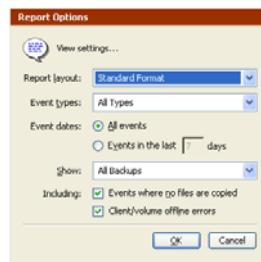
Use the options to customize the Backup Report.

Working with the Backup Report

The Backup Report is a database of backup events. Each time Retrospect completes a backup it adds a new backup event to its database. For each combination of source, destination and script, it saves all unsuccessful backup attempts and the latest successful backup.

When you forget a script, source, or Backup Set, Retrospect removes that item's backup events from the Backup Report database.

Forgetting Events

To remove events from the Backup Report, click the Forget Events icon from the toolbar. This brings up a dialog with which you can remove the following execution events from the report:

- All but the most recent successful backup
- All successful backups
- All unsuccessful attempts
- Events older than one week
- All execution events
- All Proactive Backup events

NOTE: The only one of these options that affects Proactive Backup events is "All Proactive Backup events."

You can delete a specific execution event from the Backup Report by right-clicking it and selecting Delete.

WARNING: Proactive Backup relies upon the Backup Report to determine when a volume was most recently backed up. If you delete an event from the Backup Report and the associated volume is a source in an active Proactive Backup script, Proactive Backup assigns a higher priority to that volume and will attempt to back it up sooner.

Finding Events in the Operations Log

Select a line from the Backup Report and click the Find in Log button to view more information about that event in the Operations Log.

Editing an Event Script

Select a line from the Backup Report and click Edit Script to open the script summary window for the script which executed and created the event.

NOTE: If you backed up a volume using an immediate operation, the Backup Report indicates that in the Script column (e.g. "Immediate Backup").

Printing or Exporting the Backup Report

To print the Backup Report, view it, then choose Print from the File menu. If you have only a portion of the report selected, only that portion will print. If you have nothing selected, the entire report will print. To export the Backup Report to a text file, view it then choose Export from the File menu.

TIP: You can set a preference option, described in "Logging Preferences" on page 271, to have Retrospect automatically export the Backup Report.

Viewing the Operations Log

The Operations Log stores any messages that are generated during an operation such as a backup or restore. You may need to review the log to find out why an operation was unsuccessful in order to diagnose problems.

To view the Operations Log, click Reports>Operations Log, or choose Log from the Window menu.

The example below shows how information appears in the Operations Log.

The log shows the following information for each successful operation.

Completed indicates the number and size of the files that were copied. If you used Retrospect's data compression feature, the log also shows compression achieved for this session.

Snapshot stored indicates the size of the volume Snapshot stored in the Backup Set.

Performance indicates the number of megabytes of information copied per minute. If verification is turned on, additional performance figures are listed for comparing.

Duration shows the total time required to complete the operation. If you clicked Pause during the operation or there were delays while you inserted media, the waiting time is shown separately. The waiting figure includes time spent during tape drive locate functions and other required functions.

Finding Items in the Log

Retrospect has commands for finding items in the Operations Log. The Operations Log's window and the Edit menu both have these commands.

Find Backward: This toolbar command prompts you to enter the text you want to search for. When you click OK, Retrospect searches the log bottom-up (from the current selection) instead of top-down, because the most recent operations are at the bottom of the log.

Find Again Backward: After you have used the Find or Find Backward command, this toolbar command searches bottom-up for the text you previously specified.

Find: This command on the Edit menu prompts you to enter the text you want to search for. When you click OK, Retrospect searches the log top-down from the current selection.

Find Next: After you have used the Find or Find Backward command, this Edit menu command continues the search from the current selection forward, or down. Upon reaching the end of the log, it continues searching from the beginning.

Find Prev: After you have used the Find or Find Backwards command, this Edit menu command continues the search from the current selection backward, or up. Upon reaching the log's beginning, it continues searching backward from the end.

Clearing the Log

To delete the contents of the Operations Log, view the log, then click the Clear Log icon from the toolbar.

NOTE: You do not have to manually clear the log, since Retrospect automatically removes old log entries when the log fills to its capacity, as defined by the log size limit preference (see page 271).

Printing or Exporting the Log

To print the Operations Log, view it, then choose Print from the File menu. If you have only a portion of the log selected, only that portion will print. If nothing is selected, the entire log will print.

Log size

+script executed

–operation began on this volume

>error occurred

📄 Operations Log

3,349 lines, using 455 K on disk

```
+    Executing Daily Backup at 2/28/2003 7:29 PM (Execution unit 1)
     To Backup Set 💾 M-W-F Backup Set...

-    2/28/2003 7:29:49 PM: Copying 📁 architecture on Drive C (C:)
     2/28/2003 7:29:55 PM: Snapshot stored, 10 KB
     2/28/2003 7:29:56 PM: Comparing 📁 architecture on Drive C (C:)
     2/28/2003 7:30:00 PM: Execution completed successfully
         Completed: 28 files, 8,436 KB
         Performance: 141.2 MB/minute (123.5 copy, 247.1 compare)
         Duration: 00:00:10 (00:00:02 idle/loading/preparing)

>        Can't access volume 📁 Users on DV_Ben Corson / iMac OS X, error -530 (backu
     2/28/2003 7:30:27 PM: Execution incomplete
     Total performance: 141.2 MB/minute
     Total duration: 00:00:10 (00:00:03 idle/loading/preparing)
```

To export the Operations Log to a text file view it then choose Export from the File menu.

NOTE: You can set a preference option, described in "Logging Preferences" on page 271, to have Retrospect automatically export the Operations Log.

Viewing Session Contents

Retrospect can report which files were copied to a Backup Set during a specific backup or archive session.

To view the contents of a Backup Set, first click Reports from the navigation bar, then click Session Contents.
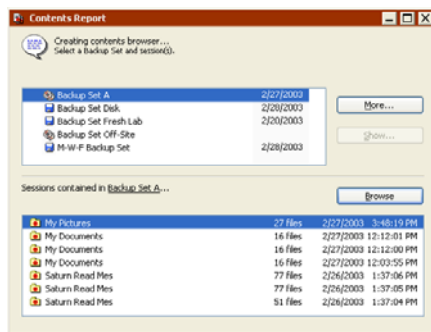
In the upper list box, select the Backup Set you want information about. (Click More to access more Backup Sets.) After you select a Backup Set, the lower list box displays the backup sessions contained within the selected Backup Set. Select the backup session or sessions you want to review.

At this point, you can choose Export from the File menu to export the list to a text file, or click Browse. When you do the latter, a browser window appears listing the files and folders that were backed up during the session or sessions you selected.
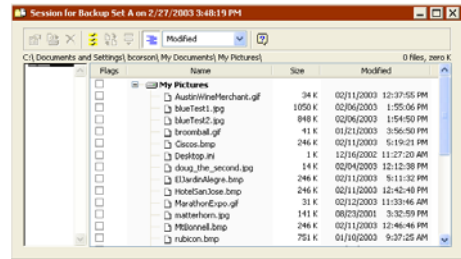
You can print the list, export it to a text file, search for specific files, get the properties of specific files, retrieve specific files, or change the view format from the browser window's toolbar. You can view browser windows for multiple sessions at the same time by performing the same steps and selecting multiple sessions. When exporting, Retrospect exports the fields in the following order, regardless of the view format: file name, size, create date, create time, modify date, modify time, backup date, backup time, Mac OS type, Mac OS creator, Backup Set, and path.

For information about using the browser window and menus, see "Browsing" on page 286.

REPORTSWATCHER

Intended primarily for large sites with multiple backup computers, ReportsWatcher is a stand-alone utility that converts Retrospect Backup Reports into HTML summaries for viewing from a web browser. Used in conjunction with Retrospect's feature to automatically export the Backup Report to a custom location, ReportsWatcher allows you to monitor one or more backup computers from any computer with a web browser.

Installing ReportsWatcher

When you install Retrospect using the default method (Recommended), the ReportsWatcher application is automatically installed. If you chose to do a custom install that did not include ReportsWatcher, you can install it now.

To install ReportsWatcher:

1. Locate and launch the Retrospect InstallShield Wizard (setup.exe).

2. Click Next.

3. Select the Modify radio button and click Next.

4. Make sure ReportsWatcher is selected for installation, then click Next.

5. Click Install.

6. Click Finish to exit the wizard.

The ReportsWatcher folder is now available. The default install location is:

..\Program Files\Retrospect\Retrospect 7.5\ReportsWatcher

Launching ReportsWatcher

Go to Start>Tqzkq Retrospect>ReportsWatcher. You can also double-click the watcher.exe file in the ReportsWatcher folder.

Because ReportsWatcher's job is to continuously monitor updated reports and automatically generate a master report from them, it should always be running.

TIP: Add a shortcut for Watcher.exe to the Start menu's StartUp (or Startup) folder so that ReportsWatcher opens automatically whenever the computer starts up.

Configuring Retrospect for ReportsWatcher

In order to take advantage of the benefits of ReportsWatcher, you must configure some Retrospect settings.

To configure Retrospect:

1. At each backup computer, open Retrospect and go to Configure>Preferences.

2. Select the Logging preferences from the Notification category.
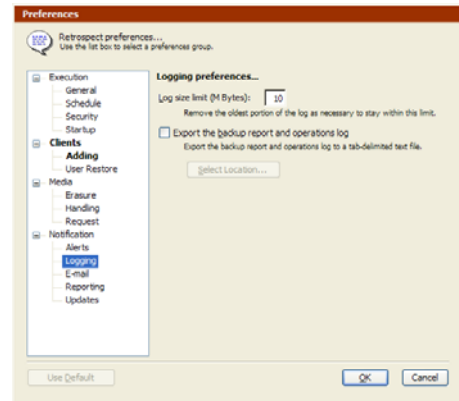
3. Turn on the option to export the Backup Report.
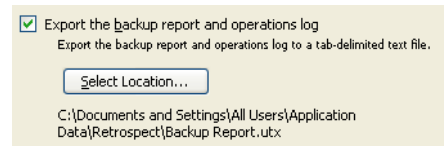
4. Click the Select Location button.

5. Browse to a location where you want Retrospect to save the Backup Report.

NOTE: If you are gathering Backup Reports for multiple backup computers, this location must be the same for all of them. Therefore make sure you select a network location accessible to all backup computers and workstations.

6. Specify a name for the exported Backup Report.

NOTE: If you are gathering reports for multiple backup computers, make sure each one uses a unique file name.

7. Click Save.

Configuring ReportsWatcher

After configuring Retrospect to automatically export the Backup Report for each backup computer, you must configure ReportsWatcher to gather those reports and generate a summary HTML report.

To configure ReportsWatcher:

1. Open ReportsWatcher.
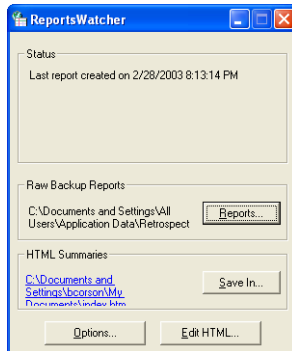
2. Click the Reports button and browse to location where Retrospect Backup Reports are stored.

This location was specified in "Configuring Retrospect for ReportsWatcher".

3. Choose any report in the folder and click Open.

NOTE: *All* reports in the folder (not just the one you choose here) will be included in the Backup Report summary.

4. Click the Save In button and specify a folder in which to save the HTML summaries.

Make sure this location is accessible to all users who will need to view the Backup Report Summary.

5. Click Save.

6. Click the Options button to change ReportsWatcher's update time interval or other options. Click OK when done.
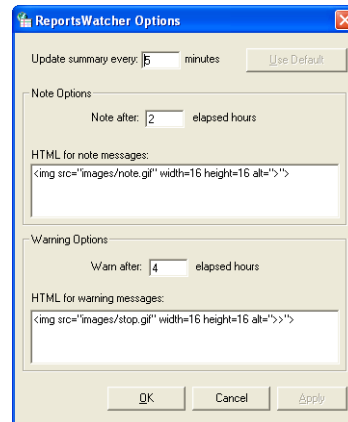
7. Click the Edit HTML button to change ReportsWatcher's HTML code.
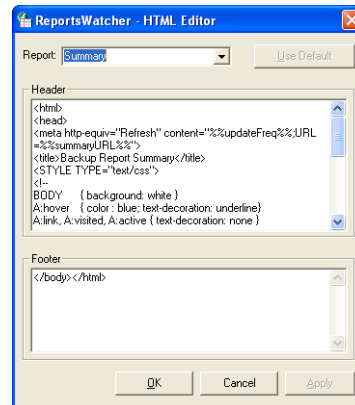
You can edit the HTML for each of the five different report types. Click OK when done.

Leave ReportsWatcher open in order for it to continuously monitor reports.

Viewing the Report

You can view the report on any computer with a web browser and access to the location where the HTML summaries are saved (as specified in "Configuring ReportsWatcher").

Browse to the HTML summaries folder and open the index.htm file. The index summarizes available reports. It has a variety of report for-

mats. To view details of a particular backup computer's report, click the report name. To view details of successful backups, failed backups, or volumes never backed up, click the numbers in the appropriate table cells.

Customizing the Report

ReportsWatcher is a Visual Basic application and its source code is included in the ReportsWatcher folder.

If you know Visual Basic, you can edit the source code to customize ReportsWatcher for your needs.

EXECUTION OPTIONS

Retrospect has many options you can set to determine how your backup, duplicate, archive, transfer, and restore operations (immediate and scripted) are executed. For example, you could set a backup script to turn on software data compression and synchronize client computer clocks. You can set options while setting up an immediate operation or while editing a script. Execution options are local rather than global, so they apply only to the current operation or script, not to all operations and scripts.

Retrospect also has global program preferences that affect all executions. See "Retrospect Preferences" on page 263 for more information.
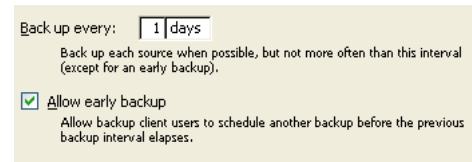
To set options for an immediate operation or a script, click the Options button in the summary window, then click More Choices to view a complete list of available options grouped by category. You can display the options for each category by clicking the category name in the list.

To turn an option on or off, click its checkbox or radio button. Some options use time and date controls, and others let you enter numbers or text. If any options in a category have been changed from their default settings, the catego-

ry name is shown in boldface. Clicking Use Default reverts all visible options to their default states. Clicking Fewer Choices returns you to the basic Options window.

Proactive Backup Interval Options

These options are available only with Proactive Backup scripts, which are described in "Proactive Backup Scripts," which starts on page 140.

Back up every: n days/hours: This time interval, which is one day by default, specifies the minimum time between backups. Each source is backed up when possible, according to the priority of need, but not more often than this interval unless the client user initiates a backup.

Allow early backup: When this option is on, which is the default, client users may initiate backups from their Retrospect Client control panels, overriding the backup interval. A request for an early backup does not necessarily immediately move the user's volume to the top of the priority list. Other sources are taken care of before Proactive Backup polls the client and learns of the early backup request, at which time Proactive Backup backs up the client source volumes.

Proactive Backup Countdown Options

These options are available only with Proactive Backup scripts.
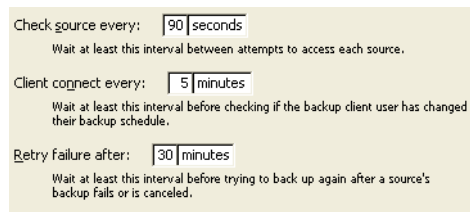
Countdown time: Retrospect gives client users advance notice of when a backup is about to begin, counting down the time specified here. The default time is twenty seconds. (Enter zero to make Retrospect skip the countdown.) When it is going to back up a source from a client computer, Retrospect puts up a dialog on the client. This dialog displays the countdown message (see below) and offers buttons to defer the backup to a later time or bypass the countdown and immediately begin backing up. If the client user does not take any action Retrospect backs up when the countdown reaches zero.

Countdown message: The text in this box is shown to a client user when a backup is about to begin, according to the countdown time option. Retrospect will replace the text "%%script%%" with the name of the script it is executing.

Proactive Backup Polling Options

These options are available only with Proactive Backup scripts.

Check source every: [90] seconds
   Wait at least this interval between attempts to access each source.

Client connect every: [5] minutes
   Wait at least this interval before checking if the backup client user has changed their backup schedule.

Retry failure after: [30] minutes
   Wait at least this interval before trying to back up again after a source's backup fails or is canceled.
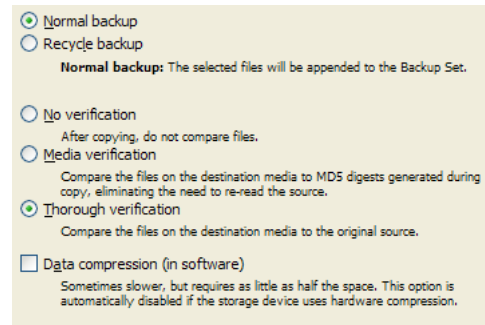
Check source every: n seconds/minutes: Retrospect uses this time interval, which is ninety seconds by default, to check whether a source is available for backup. Retrospect does not check sources while a backup is in progress.

Client connect every: n seconds/minutes: Retrospect uses this time interval, which is five minutes by default, to access a client to check whether the user has changed the backup schedule or requested an early backup. Retrospect does not connect to clients while a backup is in progress.

Retry failure after: n minutes/hours: After a backup has failed or was canceled, Retrospect waits at least this long, thirty minutes by default, before again trying to back up a source.

Backup Execution Options

These options are available only with backup operations and Proactive Backup scripts.

⊙ Normal backup
○ Recycle backup
   Normal backup: The selected files will be appended to the Backup Set.

○ No verification
   After copying, do not compare files.
○ Media verification
   Compare the files on the destination media to MD5 digests generated during copy, eliminating the need to re-read the source.
⊙ Thorough verification
   Compare the files on the destination media to the original source.

☐ Data compression (in software)
   Sometimes slower, but requires as little as half the space. This option is automatically disabled if the storage device uses hardware compression.

Normal backup: Only available with immediate backups, this option makes Retrospect perform a Normal (progressive) backup, as described in "Normal Backups" on page 24.

Recycle backup: Only available with immediate backups, this option makes Retrospect perform a Recycle backup, as described in "Recycle Backups" on page 25.

NOTE: For scripted backups, you can select a Normal or Recycle backup when you schedule the script. See "Common Scheduler Elements" on page 135 for more information.

Verification: Although verification increases the time it takes for a backup to complete, it ensures that information is correctly written to the Backup Set. Retrospect provides two verification methods:

- *Thorough verification* ensures files are copied correctly by comparing files in the destination Backup Set with the original source files after the backup is performed. If the backup spans multiple tapes, CD/DVDs,

or disks, you must reinsert all members to which data has been written.

- *Media verification* compares the files in the destination Backup Set to MD5 digests generated during the backup. This methods *does not* involve re-reading the source files, and as a result, it does not identify potential problems that would be found using Thorough verification. Media verification does have some benefits however. It can be faster than Thorough verification and also imposes fewer demands on the source volumes since Retrospect does not need to rescan them after the backup. In addition, during backup operations, Retrospect performs ongoing Media verification, which means that you do not have to reinsert Backup Set media for backups that span media.

NOTE: The Media verification option is not available if you disable Retrospect's "Generate MD5 digests during backup operations" preference. See "Verification Preferences" on page 270 for more information.

Verification scripts and the Verify Media command both use Media verification, whenever possible, to verify Backup Set media. See "Scripted Verification" on page 132 and "Verifying Backup Set Media" on page 305 for more information.

NOTE: Verification scripts and Verify Media *do* require you to reinsert media when verifying backups that span media.

Data compression (in software): Data Compression saves space in the Backup Set by compressing files before copying them into the Backup Set. Files are automatically decompressed back to their original state when restored. Compression savings achieved during an operation are reported in the status window and the Operations Log. The amount of compression savings you can expect depends on the types of files you are compressing. Text files

compress substantially; application and system files do not. Backups using data compression are slower than those without, as are restores.

When copying to a tape device that has built-in compression, Retrospect automatically turns off software compression in favor of the faster hardware compression. Retrospect uses its built-in compression filter to identify files that are already compressed (such as those compressed with a utility such as WinZip) so it will not attempt to re-compress them with software data compression. The Data Compression option is off by default.

Archiving Execution Options

These options are available only with archiving operations.
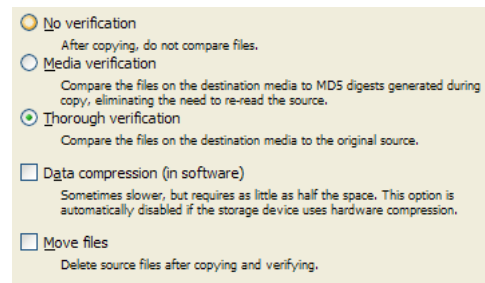
Archive operations include Verification and Data compression options, as described in "Backup Execution Options", and Move files. An archive is just like a backup unless you move files.

Move files: This option deletes files from the source volume after they have been copied. If Thorough or Media verification is turned on and the files do not match exactly, the originals will not be deleted. Do not turn on the move files option without also turning on the Thorough verification option. You should perform at least one additional verified archive, backup, or duplicate before deleting files from the source. Retrospect cannot move files from a client computer if its Retrospect Client control panel has

been set to allow read access only. By default, this option is off.

A related option is described in "Files Execution Options" on page 239.

TIP: Before you use the Move files option, first archive to a different Backup Set by copying without moving. This provides an extra measure of safety should one Backup Set become unusable.

See "Archiving Tips" on page 68 for more information about archiving.

Duplicate Execution Options

These options are available only with duplicate operations.

Thorough Verification: This is the same option described in "Backup Execution Options" on page 237, Since Duplicate operations do not involve Backup Set media, they do not have a Media Verification option.

Update backup report: When this option is checked, Retrospect treats the duplicate operation like a backup and adds or changes information in the Backup Report.

Files Execution Options

These options are only available with duplicate, archive, and restore operations.

Move files: This option, which is only available for duplicate operations, deletes files from the Source volume after they have been copied. If Thorough verification is turned on and the files

do not match exactly, the originals will not be deleted. Do not turn on the move files option without also turning on the Thorough verification option. You should perform at least one additional verified archive, backup, or duplicate before deleting files from the source. Retrospect cannot move files from a client computer if its Retrospect Client control panel has been set to allow read access only. By default, this option is off. Also see the related files option below.

NOTE: Archive operations also include a Move files option. See "Archiving Execution Options" on page 238.

On Move, don't delete empty folders: This option is only available for archive and duplicate operations. It keeps folders that become empty as a result of the move instead of automatically deleting them. By default, this option is off.

Update modify dates: This option is only available for restore operations. It causes Retrospect to set the modification date and time of restored files to the current date and time. By default, this option is off.

Transfer Execution Options

These options are available only with Backup Set and Snapshot Transfer operations, whether scripted or initiated from the Tools menu on the navigation bar.

☑ Copy Snapshots
  Copy all Snapshots from the source Backup Set to the destination. This will not overwrite existing Snapshots.

☑ Media verification
  Compare the files on the destination media to MD5 digests generated during copy.

☐ Data compression (in software)
  Sometimes slower, but requires as little as half the space. This option is automatically disabled if the storage device uses hardware compression.

☐ Recycle source Backup Set after successful transfer
  The source Backup Set is recycled if the transfer operation completes without any errors.

☐ Transfer any needed intermediate database Snapshots.
  Transfers all full, differential, and log backups required to bring the database completely up to date as of the selected database Snapshot date and time.

Copy Snapshots: This option is only available for Backup Set transfers. It copies all of a Backup Set's Snapshots to the destination Catalog and media. This option is on by default. If you turn this option off, Retrospect copies all the files from a Backup Set's Snapshots, but not the Snapshots themselves.

WARNING: Tqzkq generally recommends leaving this option set to the default. If you turn Copy Snapshots off, you can only restore by search (not by Snapshot) and cannot restore the System State or security information.

Media Verification: This option compares the files in the destination Backup Set to MD5 digests generated during the transfer. Since Transfer operations involve only Snapshots and Backup Sets, Thorough Verification is not an option.

NOTE: This option is available even if you disable Retrospect's "Generate MD5 digests during backup operations" preference, since it relies on MD5 digests generated during the *transfer*, not the original *backup*.

Data compression (in software): Data compression saves space in the destination Backup Set by compressing files before copying them. Files are automatically decompressed back to their original state when restored. Compression savings achieved during an operation are reported in the status window and the Operations Log. The amount of compression savings you can ex-

pect depends on the types of files you are compressing. Text files compress substantially; application and system files do not. Transfers using data compression are slower than those without, as are restores.

Retrospect uses its built-in compression filter to identify files that are already compressed (such as those compressed with a utility such as Win-Zip) so it will not attempt to re-compress them with software data compression.

When copying to a tape device that has built-in compression, Retrospect automatically turns off software compression in favor of the faster hardware compression. The Data Compression option is off by default.

Recycle source Backup Set after successful transfer: Select this option to recycle to source Backup Set(s) after a successful transfer. Recycling clears the Catalog File contents of a Backup Set so it appears that no files are backed up. The next time you use the recycled Backup Set as a destination, Retrospect looks for the first media member of the Backup Set, erases it, then copies files to it. Since no files exist in the Backup Set, all selected files are copied.

WARNING: Make sure you can afford to lose all data on the source Backup Set before recycling it.

Transfer any needed intermediate database Snapshots: If your source includes a database Snapshot from a backup type other than a full backup (e.g., log, incremental, or differential), select this option transfer all backups required to bring the database completely up to date as of the selected database Snapshot date and time. This eliminates the need to manually transfer multiple Snapshots.

Restore Database Options
This option is only available when restoring SQL or Exchange databases.

☑ Restore any needed intermediate Snapshots.
Restores all full, differential, and log backups required to bring the database completely up to date as of the selected Snapshot date and time.

Restore any needed intermediate Snapshots:
If you select a database Snapshot from a backup type other than a full backup (e.g., log, incremental, or differential), Retrospect will restore the most recent full backup and any needed intermediate backups before it restores the selected Snapshot. This eliminates the need to manually restore multiple Snapshots.

You can change this behavior by turning off this option. In most cases you will want to leave this option set to the default.

Retrieval Execution Options

These options are only available during an immediate restore by searching for current or older files.

☐ Only most recent versions
Find only the most recent version of each file when searching. Older versions are ignored.

☐ Minimal folder structure
Restore files using as few folders as necessary.

Only most recent versions: Of files which match the search criteria, Retrospect uses only those most recently added to the Backup Set. It ignores files from older sessions. By default, this option is off, which makes Retrospect use matching files from older *and* most recent sessions.

Minimal folder structure: Restores files to their original folders, in the minimum required hierarchy. Empty folders are not restored. This option is off by default.

Catalog File Execution Option

This option is available with all types of operations except duplicate, restore, and transfer.

☑ Save source Snapshots for restore
Snapshots permit disks to be automatically restored to their exact state as of the backup.

Save source Snapshots for restore: This option directs Retrospect to save a volume Snapshot to the Catalog, replacing the old Snapshot, if any, and to save another copy of the Snapshot onto the backup media. By default, this option is on.

NOTE: Snapshots are an important, fundamental feature of Retrospect, described in detail in "Snapshots" on page 26. Turning off this option has consequences described in "What are the consequences of not saving Snapshots to save time and space?" on page 330.

Client Execution Options

These options are available with all types of operations except restore and transfer, and these options apply only when backing up Retrospect client computers.

☐ Byte-by-byte file comparison
Much slower, but pinpoints the exact location of the comparison failure.

Speed threshold (K Bytes/second):   [0]
Do not back up a client and log an error if the initial connection speed between the client and backup server does not exceed this value.

Execution performance threshold (M Bytes/minute):   [0]
Stop backing up a client and log an error if execution performance drops below this value.

☐ Synchronize clock
Synchronize the backup client's clock to match the clock of this computer. Ignored if the client is set to Read Access Only.

Byte-by-byte file comparison: This option overrides Retrospect's fast client compare, verifying files the same way Retrospect does for local backups. When this option is turned off, Retrospect uses a faster, checksum-based technique to verify copied files. Both methods reliably compare backed-up data to the original files. By default, this option is off and you should keep it off.

NOTE: This option has no effect if verification is turned off, or if Media verification is selected.

Speed threshold: This option, which is available only with scripts, is useful for preventing backups which would be too slow. The number

you enter here determines the minimum acceptable rate at which the client computer is accessed. If, upon testing the network connection to the client prior to the operation, Retrospect finds the network or client is not working fast enough, it will terminate the operation and log an error.

This option is useful, for example, for preventing Proactive Client Backup from trying to back up a notebook computer volume when its user dials in to connect with the LAN.

Retrospect checks the client connection speed only once, as an operation starts. The performance threshold option described below is a more comprehensive control.

Execution performance threshold: This option, which is available only with scripts, is useful for halting backups which are too slow. This allows queued backups and other operations to execute rather than wasting time on a hopelessly slow client. The number you enter here determines the minimum acceptable data copying performance, in megabytes per minute, for the client. Retrospect continually measures and updates its performance with the client. An execution that initially performs acceptably may later be halted by Retrospect if its performance drops below the threshold. If the threshold number is set to zero, which is the default, Retrospect does not evaluate execution performance and will not halt an execution for lack of performance.

Synchronize clock: This option sets the date and time on each client computer to match the clock on the backup computer. This is useful to get times and dates to agree and is especially useful when changing to and from daylight savings time. Retrospect cannot synchronize a client computer's clock if its Retrospect Client control panel has been set to allow read access only. By default, the synchronize option is off.

Matching Execution Options

These options are available with all types of operations except duplicate and restore.

Match source volumes to Catalog File: This option directs Retrospect to identify previously backed up files during Normal backups. Retrospect compares the files on the source volume to file information in the Backup Set Catalog. The Windows file matching criteria are name, size, creation date, and modify date. The Mac OS file matching criteria are name, size, type, creator, creation date, and modify date. The UNIX and NetWare file matching criteria are name, size, and modify date. Retrospect considers a file already backed up if all of these criteria match. When you view the preview browser while setting up an immediate backup, files that have already been backed up are preceded by a diamond symbol.

Archive operations have the matching option off by default, which results in archiving all selected files, regardless of whether they are already in the Backup Set. Unless you turn on the Move files option, matching is the only difference between archive and backup scripts.

NOTE: For transfer operations, this option is called "Match source Catalog File to destination Catalog File". When selected, Retrospect only copies those files and Snapshots not already in the destination Catalog File.

Don't add duplicates to Backup Set: This option works with the "Match source volumes to Catalog File" option to prevent previously backed up files from being added to the Backup Set again. Select both of these options when you

want to perform a standard Progressive Backup; that is, you only want new or modified files copied to the Backup Set. If this option is deselected, Retrospect adds all files, including previously backed up files, to the Backup Set every time a Normal Backup is performed. By default, this option is on (except for Archive operations) and you should keep it that way unless you have a specific need to change it.

Match only files in same location: This option is only available if "Match source volumes to Catalog" is selected. It makes Retrospect more strictly match otherwise "identical" files from a source to a destination. (Normally, files are considered identical files when they have the same criteria described above in "Match source volumes to Catalog File".) This option adds another criterion; files must also come from the same volume.

By default, this option is off and you should keep it that way unless you have a specific need to change it.

Verification Execution Options

These options are only available with verification scripts.

Verify only backups not previously verified: Since Retrospect keeps track of which backups it has verified and which it has not, this default option is the one you should use most of the time. In general, verification scripts with this option selected should require less time than verification script using the "Verify entire Backup Set" option.

NOTE: If none of the backups in Backup Set have been verified, this option has the same effect as "Verify entire Backup Set".

Verify entire Backup Set: This option verifies the entire Backup Set. If that Backup Set spans multiple media members, you may have to insert media as Retrospect requests it. You can choose this option if you have reason to believe there might be problems with older Backup Set media, although using the Verify Media command can accomplish the same goal without a script. See "Verifying Backup Set Media" on page 305 for more information.

Schedule Execution Option

This option is only available for scripts (not including Proactive Client Backup scripts).
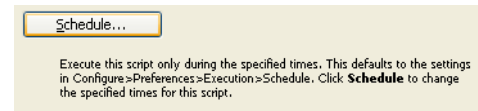
Click Schedule to define a time period during which this script may execute. The default schedule reflects the global schedule preference, described in "Schedule Preferences" on page 264.

Sharing Execution Option

This option is available with all types of operations except restore and transfer. It is off by default.
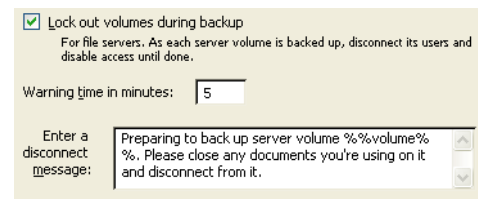
Lock out volumes during backup: This option disconnects users connected to the backup computer through Microsoft Networking and prevents them from using a shared volume during backup. When you check this option, you can enter a warning message that is displayed to users before they are disconnected. (Windows NT/2000/XP users automatically receive warn-

ing messages. Windows 98 users receive warning messages if they are running Winpopup.exe; Windows 95 and Macintosh users do not receive warning messages.) You can also specify how many minutes advanced warning users will be given. This option will lock out users only if you are running Retrospect on the server itself; it does not apply to clients.

The lock out option behaves differently for Services For Macintosh network volumes on NT Servers and Windows 2000 Servers. All Services For Macintosh shared volumes are locked out at once, even if they are not all actively being backed up. All are locked while any one is backed up with the sharing lock out option enabled. By default, this option is off.

Media Execution Option

This option is available with backup, archive, and transfer operations, as well as with verification scripts. This option is *not* available with Proactive Backup, restore, or duplicate operations.

> ☐ Eject tapes and discs when script is complete
> Eject any accessed tapes or discs when script is complete.

Eject tapes and discs when script is complete
Once a script has run, this option tells Retrospect to eject any tapes or discs that it accessed during the script.

Windows System Options

These options are available with all types of operations except transfers. The specific options change according to the operation No option in this category affects UNIX, NetWare, or Macintosh clients.

> ☑ Back Up System State
> Back up system configuration information, such as the registry, when the Windows volume is backed up.

Windows System options for a backup or archive operation.

> ☑ Duplicate System State
> Duplicate selected system configuration information, such as the registry, when the Windows volume is duplicated.
> ☐ Ignore encrypted file verification errors
> Don't report verification errors for encrypted files on NTFS volumes.

Windows System options for a duplicate operation.

> ☐ Restore System State
> Restore system configuration information, such as the registry, when the Windows volume is restored.
> ☐ Restore security information
> Restore security information for NTFS volumes.
> ☐ Restore security information for matched files
> Restore security information for NTFS volumes when the files appear to be same as in the Backup Set and does not neeed to be restored.
> ☑ Set archive attribute
> Set the archive flag of a Windows file when it is restored.

Windows System options for a restore operation.

System State: provides the option to copy the Windows registry, COM+, active directory, and certificate services when the Windows folder is included in the file selection criteria. Retrospect stores the information in the Snapshot and it must be restored with a restore method using the Snapshot.

This option is on by default for backup, duplicate, and archive operations. It is also on by default when you are restoring an entire volume.

NOTE: If you are backing up or duplicating in Wizard Mode and choose not to copy "Operating System and Applications" files, Retrospect automatically disables the "Back Up/duplicate System State" option. In Advanced Mode, the option is always on by default, no matter what file types you select.

In order to restore the System State, the source Snapshot must contain a backed up System State and the destination must be a system volume.

In order to duplicate the System State, the source and destination must both be system vol-

umes (i.e., they must both include System State information).

NOTE: You must have Administrator or Backup Operator privileges to copy System State information under Windows NT/2000/XP/2003.

Ignore encrypted file verification errors: in duplicate operations, which is off by default, causes Retrospect to ignore verification errors with encrypted files on NTFS volumes.

Restore security information: is only available for restore operations (excluding Find Files restores). When this option is enabled, Retrospect restores NTFS security information for all the restored folders and for the restored files that did not already exist on the destination.

If the same file exists in the source Snapshot and on the destination, and the only difference between the two files is their security information, the file on the destination will retain its security information.

NOTE: Security information can only be restored if it was backed up. See "Windows Security Options".

Restore security information for matched files is only available for restore operations (excluding Find Files restores). When this option is used in combination with the previous option, Retrospect restores NTFS security information for *all* the restored files and folders.

If the same file exists in the source Snapshot and on the destination, and the only difference between the two files is their security information, the file on the destination is replaced with the file from the Snapshot.

NOTE: Security information can only be restored if it was backed up. See "Windows Security Options".

Set archive attribute: Retrospect can set the archive attribute during restore operations (including Find Files restores). When selected, this option causes Retrospect to set the archive attribute for restored files.

Setting the archive attribute ensures that Retrospect backs up file security information for the restored files the next time they are backed up (and you have selected the option to back up file security information). See "Windows Security Options" for more information.

Windows Security Options

These options, available with backup (including Proactive Backup), duplicate, and archive operations, allow you to copy NTFS file and folder security information from servers and workstations. The specific options vary depending on the type of operation.

NTFS security permissions are a feature of Windows operating systems that allows you to restrict or permit access to files and folders based on user or group membership. These permissions are only available on disks that are formatted as NTFS.

It can take Retrospect a significant amount of time to copy security information for all the files and folders on a workstation or server. You can improve performance by deciding to copy only the security information you really need. But, you should be aware that when you restore files and folders for which you did not copy security information, those files and folders will be available to any user with access to the computer to which you restored. If you are unsure about whether to copy security information or not, use Retrospect's default settings.

Retrospect stores NTFS security information in its Snapshots and therefore you must restore by Snapshot in order to restore security information. To restore NTFS file and folder security information, choose a Snapshot from which to

restore, then use the restore security information options described in Windows System Options.

NOTE: You must back up folder security information in order to do a complete restore.
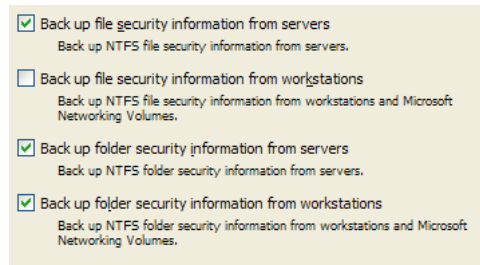
Windows Security options for a backup and archive operations.
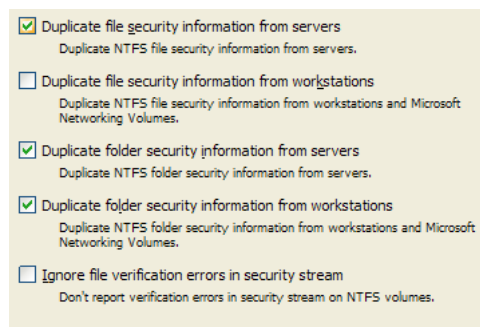
Windows Security options for a duplicate operation.

Back up file security information from servers: This option is on by default and causes Retrospect to back up NTFS *file* security information from source computers running server operating systems. When this option is enabled, Retrospect copies file security information for all the files it backs up.

In addition, if a file has new security information since the last backup, but has not changed in any other way, Retrospect copies the new security information for that file. Since Windows sets the archive attribute when a file's security information changes, Retrospect uses the archive attribute to identify these files.

If the archive attribute has been set since the last time Retrospect backed up a file from the same location, Retrospect copies the file's security information, even if nothing else about the file has changed.

NOTE: Retrospect can even keep track of archive attribute changes across Backup Sets. For example, if Backup Set A includes a copy of a file with new security information and Backup Set B does not, the file (and its security information) will get copied during the next backup to Backup Set B.

Back up file security information from workstations: This option is off by default. When it is enabled, Retrospect copies NTFS *file* security information from source computers running non-server operating systems, as well as from Microsoft Networking Volumes. When this option is enabled, Retrospect copies file security information for all the files it backs up.

As with the "Back up file security information from servers" option, Retrospect uses the archive attribute to identify and backup files with new security information.

Back up folder security information from servers: This options is on by default and causes Retrospect to copy NTFS *folder* security information from source computers running sever operating systems. When this option is enabled, Retrospect copies folder security information for all the folders on the source.

Back up folder security information from workstations: This option is on by default and causes Retrospect to copy NTFS *folder* security information from source computers running non-server operating systems, as well as from Microsoft Networking Volumes. When this option is enabled, Retrospect copies folder security information for all the folders on the source.

NOTE: If you are backing up in Wizard Mode and choose not to copy "Operating System and Applications" files, Retrospect automatically disables the "Back up folder security information from workstations" option. In Advanced Mode, the option is always on by default, no matter what file types you select.

Duplicate file security information from servers: This option is on by default and causes Retrospect to copy NTFS *file* security information from source computers running server operating systems. When this option is enabled, Retrospect copies file security information for all the files on the source.

Duplicate file security information from workstations: This option is off by default. When it is enabled, Retrospect copies NTFS *file* security information from source computers running non-server operating systems, as well as from Microsoft Networking Volumes. When this option is enabled, Retrospect copies file security information for all the files on the source.

Duplicate folder security information from servers: This options is on by default and causes Retrospect to copy NTFS *folder* security information from source computers running sever operating systems. When this option is enabled, Retrospect copies folder security information for all the folders on the source.

Duplicate folder security information from workstations: This option is on by default and causes Retrospect to copy NTFS *folder* security information from source computers running non-server operating systems, as well as from Microsoft Networking Volumes. When this option is enabled, Retrospect copies folder security information for all the folders on the source.

NOTE: If you are duplicating in Wizard Mode and choose not to copy "Operating System and Applications" files, Retrospect automatically disables the "Duplicate folder security

information from workstations" option. In Advanced Mode, the option is always on by default, no matter what file types you select.

Ignore file verification errors in security stream: This options is only available for duplicate operations and is off by default. When enabled, this option causes Retrospect to ignore verification errors with security streams on NTFS volumes.
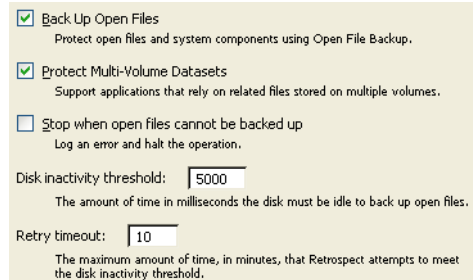
Windows Open Files Options

These options are available with all types of operations except restore and transfer.

NOTE: Open File backup is an add-on product to the main Retrospect application. If the backup computer is installed with Retrospect Disk-to-Disk, Small Business Server, Single Server, or Multi Server and you have a license code for Open File Backup, you can back up open files on Windows 2000, NT 4.0, and XP computers. To back up open files on a Windows XP computer, it must have an NTFS volume. Click Configure>Licenses to view your current licenses or purchase new ones.

Open Files can be backed up, archived, and duplicated. If you have the Open File Backup add-on, this option is on by default.

NOTE: To restore files that were backed up with Open File Backup, make sure to close or stop the application that uses the open files on the destination volume.

Back Up/Duplicate Open Files allows Retrospect to copy busy files which could otherwise not be copied. It is on by default.

Protect Multi-Volume Datasets backs up or archives applications that store files on more than one volume.

Stop when open files cannot be backed up/duplicated causes Retrospect to halt the operation if the retry timeout occurs or if the system configuration does not support Open File backup. When this option is off, Retrospect backs up or duplicates all other files (i.e., files that are *not* open).

Disk inactivity threshold is the amount of time Retrospect waits for the source disk to be idle in order to proceed with Open File Backup. When the threshold is reached, Retrospect waits again until the retry timeout occurs. The default threshold is 5000 milliseconds.

Retry timeout is the total amount of time allotted for Retrospect to monitor disk inactivity, looking for its opportunity to copy open files. When it times out Retrospect either halts the operation immediately or continues without Open File Backup, depending on the above "Stop" option. The default time is 10 minutes.

Windows Outlook Options

These options are available with all types of operations except restore and transfer.

Force backup of Microsoft Outlook data causes Retrospect to close Microsoft Outlook in order to back up Outlook data files. After Retrospect copies the files, you must manually relaunch Outlook.

Windows SQL Server Options

Retrospect has some SQL Server options that are available only for backup operations.

Backup type lets you specify the type of SQL database backup to perform. By default, Retrospect performs a full backup.

Other SQL Server options are only available when restoring SQL databases.

Use new database name for restore database lets you specify a new name for the restored database.

Use custom path for restore database data and log files lets you specify a destination path for the restored files.
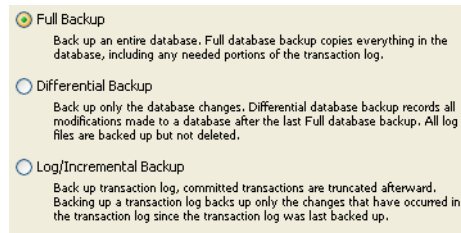
Restore only records before point in time lets you specify a time and date for restoring transactional logs. Retrospect will only restore records from before the specified date and time.

Make SQL database operational tells the SQL server to make the database operational af-

ter the restore operation is complete. Turn this option off only if you need to restore additional differential or transactional Snapshots after the current operation has executed.

Windows Exchange Server Options

Retrospect has some Exchange Server options that are available only for backup operations.
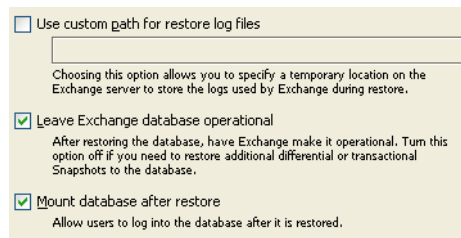
Backup type lets you specify the type of Exchange database backup to perform. By default, Retrospect performs a full backup.

Other Exchange Server options are only available when restoring Exchange databases.

Use custom path for restore log files lets you specify a destination path for the restored files.
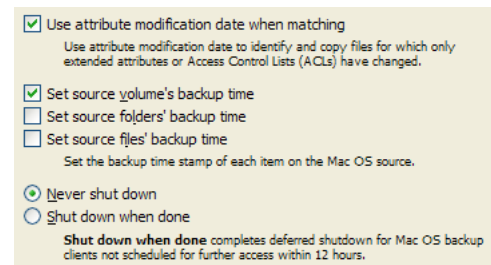
Leave Exchange database operational tells the Exchange server to make the database operational after the restore operation is complete. Turn this option off only if you need to restore additional differential or transactional Snapshots after the current operation has executed.

Mount database after restore allows users to log into the database after it is restored. Turn this option off only if you need to restore addi-

tional differential or transactional Snapshots after the current operation has executed.

Macintosh Client Options

These options are available with all types of operations except transfers. The specific options change according to the operation. No option in this category affects Windows, NetWare, or UNIX clients.

Macintosh Client options for a backup or archive operation.

Macintosh Client options for a duplicate operation.

Macintosh Client options for a restore operation.
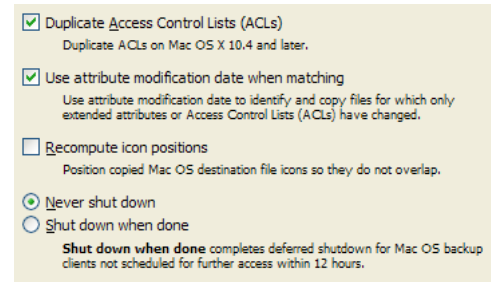
Use attribute modification date when matching: This option is available for backup, archive, duplicate, and restore operations. By default, it is enabled for all operations except

Archive (which does not match files at all un-less you choose to do so). When this option is enabled, Retrospect uses the attribute modifica-tion date to identify and copy files for which only the extended attributes or ACLs are differ-ent. For example, if you are backing up a file that was backed up previously and you modify the ACLs on that file (but make no other chang-es to it), the only way for Retrospect to know that the file is different (and therefore should be backed up again) is by looking at the attribute modification date.

NOTE: Extended attributes and ACLs are only supported on Mac OS X 10.4 and later.

Set source (volume's/folders'/files') backup time: These options, not available with dupli-cate operations, record a backup time for each source volume, folder, or file. (The Mac OS keeps track of the creation date, modification date, and backup date for each file, folder, and volume.) Using these options allows you to cre-ate selectors based on the "backup time," which is the moment execution begins. Retrospect cannot set the source backup time on a client computer if its Retrospect Client control panel has been set to allow read access only. By de-fault, the volume option is on and files and folders options are off.

NOTE: When matching files, Retrospect does not use the backup time stamp. It uses more sophisticated and flexible criteria, as described in "How Retrospect Works" on page 22.

Never shut down/Shut down when done This option specifies how Retrospect handles the Finder's Shut Down process on a client Macin-tosh after Retrospect is done with its operation.

NOTE: The desired behavior only happens when the client Macintosh is waiting for backup as described in "Execution Preferences" on page 184.

• Shut down when done completes shut down unless the client is scheduled for another

operation within the look ahead time period (see "Schedule Preferences" on page 264).

• Never shut down prevents the operation for which this option is selected from shutting down the client.

By default, the option is set to Shut down when done

Recompute Icon Positions: This option is only available for restore operations. It manipulates the positions of file and folder icons copied to a Mac OS destination to prevent overlapping of icons. By default, this option is off.

Restore Access Control Lists (ACLs)/Dupli-cate Access Control Lists (ACLs): This option is available for restore and duplicate operations. It is on by default when restoring an entire vol-ume and off by default when restoring files and folders.

NOTE: ACLs are only supported on Mac OS X 10.4 and later.

UNIX Client Options

This option is available for backup, duplicate, and restore operations only. It does not affect Window, NetWare, or Mac OS clients.

☑ Use status modified date when matching
Copy files with extended attributes if status modified date has changed.

Use status modified date when matching This option is enabled by default for backup, dupli-cate, and restore entire volume operation. It is off by default for find files restore and files and folders restores. When this option is enabled, Retrospect uses the status modified date to iden-tify and copy files for which only the extended attributes are different. For example, if you are backing up a file that was backed up previously and you modify the extended attributes on that file (but make no other changes to it), the only way for Retrospect to know that the file is dif-ferent (and therefore should be backed up again) is by looking at the status modified date.

NOTE: This option is only supported on file systems and kernels that support extended attributes.

MANAGING BACKUP SETS

Retrospect provides a number of tools to help you effectively manage your Backup Sets. Click Configure>Backup Sets from the navigation bar to view a list of current Backup Sets, organize the Backup Set list, configure, create, and delete Backup Sets, and add new members to existing Backup Sets.

Viewing the Backup Set List

To view a list of the Backup Sets currently in use by Retrospect, click Configure>Backup Sets. The Backup Sets window displays.
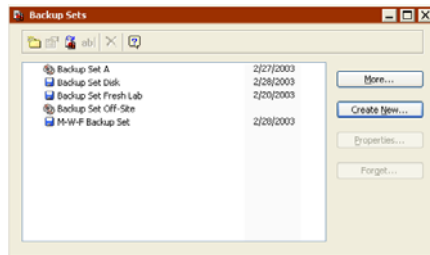
You can modify the list by:

- Creating New Backup Sets
- Recreating Old Backup Sets
- Forgetting Backup Sets

Creating New Backup Sets

To create a new Backup Set, click Create New. The process of creating a new Backup Set is described in "Creating Backup Sets" on page 252.

Recreating Old Backup Sets

If your Backup Set does not appear in the Backup Sets window, you can add it to the list using its Catalog File. To start, click More. The Access More Backup Sets window displays.
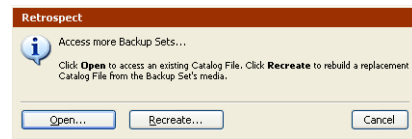
From this window you can:

- Open an existing Catalog File: If you know the location of the Backup Set's Catalog File, click the Open button. Browse to the location where the Catalog File is stored, select the file, then click Open.
- Recreate the Catalog File from the storage media: Click the Recreate button. Recreate the Catalog File as described in "Recreating a Catalog," which starts on page 302.

After you open or recreate the Catalog File, its associated Backup Set appears in the list.

Forgetting Backup Sets

You can remove a Backup Set from the Backup Set list by selecting it and clicking the Forget button. Click OK when prompted to remove the Backup Set. Forgetting a Backup Set does not affect the contents of the Backup Set, nor does it delete its Catalog File. However, it does remove the Backup Set from any scripts that use it.

As long as you don't delete the Catalog File and erase the media on which the Backup Set is stored, you can always add the Backup Set back to the list later. This process is described in "Recreating Old Backup Sets".

Organizing the Backup Set List

When you have to manage a large number of Backup Sets, you can use folders to help organize them. For example, you might want to create folders for inactive Backup Sets that you have moved to an off-site safe deposit box.

NOTE: The folders you create in the Backup Sets window are for organizational purposes only and do not exist outside of Retrospect.

To create and populate a folder:

1. In the Backup Sets window, click the New Folder icon in the toolbar.

2. Enter a name for the folder and click Create.

3. Drag and drop the Backup Set(s) you want to move into the folder.

NOTE: You can also right-click the Backup Sets you want to put in the folder and select Cut from the pop-up menu. The right-click the folder and select Paste.

Creating Backup Sets

You can create new Backup Sets from either the Backup Sets window (Configure>Backup Sets) or from the Backup Set Selection window that appears when setting up some immediate and scripted operations (e.g. specifying the destination for an Advanced Mode backup).

Click the Create New button to create a new Backup Set. The Create New Backup Set Wizard launches.

Welcome Screen

Read the information in the introductory screen, then click Next to begin creating a new Backup Set.

TIP: To skip this screen the next time you create a new Backup Set, select the check box before clicking Next.

Choosing the Backup Set Type

Click an option button to select the type of backup media you want to use for this Backup Set and click Next.
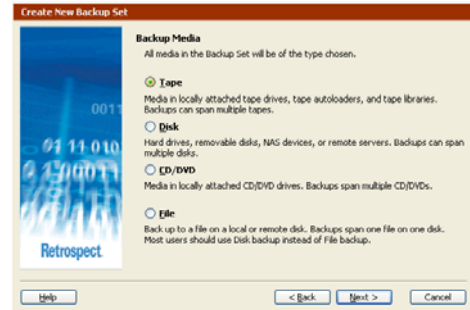
Naming Tape Backup Sets

Enter a unique and descriptive name in the Name field. Retrospect uses this name to identify both the Catalog File and the Backup Set media.

It is important to give the Backup Set a name before proceeding with any other steps.

NOTE: Once you name a tape Backup Set, you cannot rename it later.

Set the data compression option. When the Allow Hardware Data Compression check box is selected, Retrospect uses the tape drive to compress data in this Backup Set, provided that:

• The tape drive supports data compression

• The Backup Set data is not encrypted

NOTE: If you need to use both encryption and compression, specify an encryption option in the security dialog and use Retrospect's software compression option. For more information, see "Backup Execution Options" on page 237.

Set the WORM option. Select "Make this a WORM Backup Set" to create a WORM tape Backup Set. See "WORM Tape Support" on page 41 for more information.

To define multiple tape Backup Sets at once, se-lect the "Go directly to defining additional tape Backup Sets" check box and click Next.

Defining Multiple Tape Backup Sets

You can create up to five tape Backup Sets at one time.
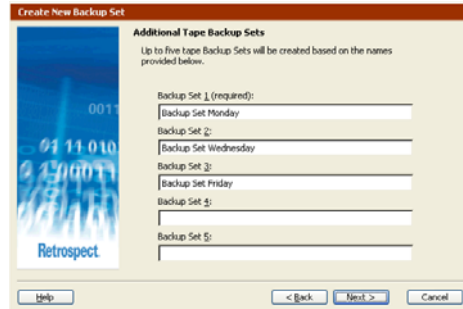
Enter a name for each Backup Set you want to create and click Next.

NOTE: All the Backup Sets defined here will have the same options (hardware compression, WORM, security, and Catalog File location).

Naming Disk Backup Sets

Enter a unique and descriptive name in the Name field. Retrospect uses this name to identi-fy both the Catalog File and the Backup Set media.

It is important to give the Backup Set a name before proceeding with any other steps.

NOTE: Once you name a disk Backup Set, you cannot rename it later.

To specify a disk:

1. Click Select.

2. Select a hard disk or removable disk to add as storage.
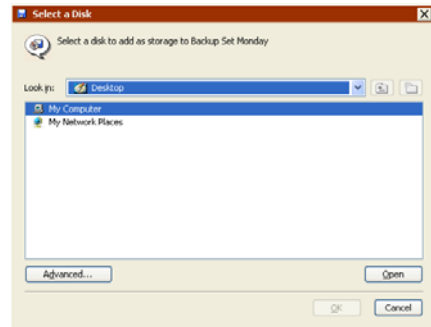
You can browse local disks and network volumes or click Advanced to specify a UNC path to the volume you want to use.

NOTE: Removable disks do not appear unless a disk is loaded in the drive.

3. Click OK.

4. Specify the maximum amount of disk space that Retrospect should use for the Backup Set data.

NOTE: This only applies to hard disks. For removable disks, Retrospect uses the entire disk.

5. Click Next.

Naming CD/DVD Backup Sets

Enter a unique and descriptive name in the Name field. Retrospect uses this name to identi-fy both the Catalog File and the Backup Set media.

NOTE: Once you name a CD/DVD Backup Set, you cannot rename it later.

Naming File Backup Sets

Enter a unique and descriptive name in the Name field. Retrospect uses this name to identi-fy both the Catalog File and the Backup Set media.

It is important to give the Backup Set a name before proceeding with any other steps.

NOTE: File Backup Sets *can* be renamed with the Windows Explorer.

If you want to save the file Backup Set data to a location other than the default, click Browse, specify the location, then click Save.

Setting Backup Set Security Options
This screen allows you to specify a password to restrict access to the Backup Set, with the option to encrypt the Backup Set data.

NOTE: Using encryption increases backup time.

Choose an option from the Backup Set Security list box:

- **None**: provides no password protection for the Backup Set and does not encrypt the Backup Set data.
- **Password only**: provides password protection for the Backup Set. Stored data is not encrypted.
- **SimpleCrypt**: provides password protection and encrypts Backup Set data using Retrospect's proprietary encryption format.
- **DES**: provides password protection and encrypts Backup Set data using the Data Encryption Standard.
- **AES-128**: provides password protection and encrypts Backup Set data using the Advanced Encryption Standard (128 bit).
- **AES-256**: provides password protection and encrypts Backup Set data using the Advanced Encryption Standard (256 bit).

WARNING: If you forget your password you cannot access your Backup Set. There is no "magic key" or "back door" to circumvent the encryption. Not even Tqzkq Retrospect Technical Support can help you.

If you set a password and want Retrospect to remember it under certain circumstances, select an option from the remember password list box.

- **Remember password for any access**: saves the password for use with all immediate and automated operations.
- **Remember password for scripted access** (default): saves the password for use with automated operations only. For example, if the Backup Set is the destination for an overnight backup script, Retrospect will not require the password to be entered manually.
- **Do not remember password for any access**: requires you to enter the password to access the Backup Set in any way. For example, you cannot back up to it or view its properties without entering the password. After you enter the password once, you do not have to enter it again until you quit and restart Retrospect.

   WARNING: Disk Backup Sets with the "Do not remember password for any access" password option selected cannot be accessed from the User Initiated Restore web page.

NOTE: You can change this setting at a later time by modifying the Backup Set's properties. See "Configuring Backup Sets" on page 255 for more information.

Grooming Options for Disk Backup Sets
These options are only available disk Backup Sets. The selection you make tells Retrospect what to do when the hard drives to which you are backing up becomes full (or uses all the disk space you allotted).

NOTE: You can change or turn off a disk Backup Set's grooming options at any time. See

"The Options tab" on page 256 for more information.

- **Ask for a new disk** When the backup drive fills up, Retrospect asks for another hard drive on which to store additional backups. All of your backups on the original hard drive are preserved.

- **Keep only the last *n* backups**: Specify the number of backups you want to preserve for each source when the backup drive fills up. Retrospect then automatically "grooms" (i.e., deletes) all the other, older backups on the hard drive to make room for new data.

- **Keep according to Retrospect's defined policy**: When the backup drive fills up, Retrospect uses its own grooming policy to delete old backups. At a minimum, Retrospect's policy retains two backups for each source. Retrospect keeps the last backup of the day for each source from the two most recent days on which each source was backed up. If the disk has enough space available, Retrospect keeps a backup of each source for every day in the last week, a backup for each week in the last month, and a backup for each previous month.

WARNING: Grooming deletes files and folders. These files and folders cannot be recovered. Before enabling grooming, make sure you have a backup policy that protects your critical files and folders.

Saving the Catalog File

Enter a location (or use the default location) to save the Catalog File that keeps track of the contents of the Backup Set.

For file Backup Sets the Catalog File and Backup Set are stored together in the location chosen earlier.
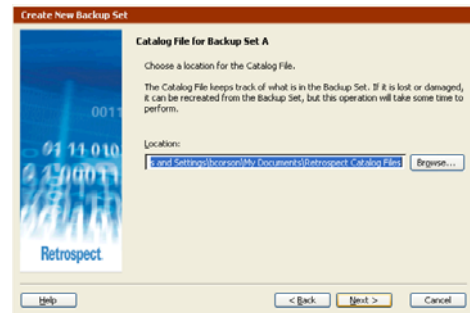
NOTE: Do not save the Catalog on a removable disk that will be used as a backup destination. Retrospect needs to access the Catalog on a readily accessible volume, preferably the local hard disk.

Finishing the Wizard

This screen includes information specific to the type of Backup Set you created. Read the information, then click Finish to exit the wizard.

For tape Backup Sets, you can select the check box and click finish to add one or more tapes in your tape drive as members of this Backup Set. See "Adding Tapes to a Backup Set" on page 260 for more information.

NOTE: This option is not available if you created multiple tape Backup Sets at one time.

Configuring Backup Sets

You can view and modify the properties of existing Backup Sets at any time. Click Configure>Backup Sets to view a list of current Backup Sets. Select the Backup Set to configure, then click Properties.

The Backup Set Properties window displays.
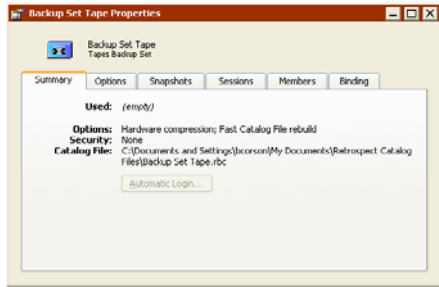
The window is divided into six tabs:

- The Summary tab
- The Options tab
- The Snapshots tab
- The Sessions tab
- The Members tab (not available for file Backup Sets)
- The Binding tab (only available for tape Backup Sets)

The Summary tab

The Summary tab displays general information about the Backup Set, including:

- **Used** shows how much space is used on the current Backup Set member and how many files are stored on that member.
- **Available** shows how much space remains on the current Backup Set member.
- **Storage** summarizes the number of media members and sessions in the Backup Set and the number of Snapshots in its Catalog File.
- **Catalog File** shows the path to the location where the Backup Set's Catalog is stored.

The Options tab

The Options tab has controls for the Catalog File, media action, and remembering passwords.

The Catalog File compression option allows you to compress the Catalog File, saving space on your hard disk.

When the Fast Catalog rebuild option is selected, Retrospect stores a copy of the Catalog File on each new media member. This greatly reduces the time required to recreate a lost or damaged Catalog File.

The Password options allow you to choose the level of password protection for secure Backup Sets. Password options are not available if you did not specify encryption or password protection when you created the Backup Set.

- Ask for any access: This option requires you to enter the password to access the Backup Set in any way. You cannot back up to it, view its properties, etc. without entering the password. After you enter the password once, you do not have to enter it again until you quit and restart Retrospect.

  WARNING: Disk Backup Sets with the "Ask for any access" password option selected cannot be accessed from the User Initiated Restore web page.

- Save for scripted access (default): This option saves the password for use with unattended scripts only. For example, if the secure Backup Set is the destination for a scripted overnight backup, Retrospect will not require the password to be entered manually.

- Save for any access: This option saves the password for all types of operations, immediate, automated, attended, and unattended. It is the equivalent of not having a password at all.

NOTE: Changes to the password access option do not take effect until you exit and restart Retrospect.

The Media Action button allows you to specify the backup action, i.e. how the storage media

will be handled the next time you perform a backup to this Backup Set. For more information on backup actions, see page 24.

- Normal continues to append data to the current Backup Set and media.
- Recycle erases and reuses the media, in addition to erasing the Catalog. This is known as resetting the Backup Set.
- New Backup Set creates a new Backup Set that expects a new medium.
- New Member requests a new member to add to the current Backup Set. New member is useful when the current member (CD/DVD, tape, or disk) is almost full and you wish to get a complete, unattended execution without changing media.
- Groom initiates a grooming operation to remove the files and folders in a disk Backup Set that are no longer required by the Backup Set's specified grooming policy. Use this option or a grooming script to delete older files and folders *prior* to the time when Retrospect requires more disk space, for example during a backup. See "Scripted Grooming" on page 131 for more information.

The Capacity button, available only with tape Backup Sets, allows you to change Retrospect's estimate of your tape capacity. The capacity estimates are used for display purposes only and do not affect how much data Retrospect will copy to a medium because it always uses all available space. Leave the default (automatic) to let Retrospect estimate the capacity, unless your media consistently get higher capacity than Retrospect estimates. To see the actual capacity, click the Members tab. Doing this for a few of your Backup Sets that have full tapes will give you a good idea of the useful capacity of your media.

Grooming options are available for disk Backup Sets only. Disk Backup Sets can be set up to au-tomatically "groom" (i.e. delete) old data to make room for new data when Retrospect finds the disk is full or hits a specified disk limit. You can either specify the minimum number of Snapshots you want to retain for each source, or use the Retrospect grooming policy. At a minimum, Retrospect's policy retains two Snapshots for each source. Retrospect keeps the last Snapshot of the day for each source from the two most recent days on which each source was backed up. If the disk has enough space available, Retrospect keeps a Snapshot of each source for every day in the last week, a Snapshot for each week in the last month, and a Snapshot for each previous month. See "Disk Grooming" on page 38 for more information.

WARNING: Grooming deletes files and folders. These files and folders cannot be recovered. Before enabling grooming, make sure you have a backup policy that protects your critical files and folders.

For more information on setting disk grooming options in the Backup Set Creation Wizard, see "Grooming Options for Disk Backup Sets" on page 254.

The Snapshots tab
The Snapshots tab shows the active Snapshots in the Backup Set Catalog File and provides basic information about each Snapshot.

- Select a Snapshot and click Properties to view the Snapshot's Backup Set, type, user, creation date and time, OS, and file system.
- Click Add to retrieve older Snapshots from the storage media. In the Snapshot Retrieval window, select a session, then click Retrieve.
- Select a Snapshot and click Forget to remove the Snapshot from the Catalog File. (The Snapshot remains on the backup media and can be retrieved later). When you forget a Snapshot from a disk Backup Set with grooming enabled, Retrospect deletes the

selected Snapshot and its associated files. (The Snapshot and files *cannot* be retrieved later).

• Select a Snapshot and click Browse to view a list of the files and folders in the Backup Set.

For disk backup Sets that have a grooming option enabled, you can select individual Snapshots to manually groom, thereby reclaiming disk space.

NOTE: When you manually groom a Snapshot, Retrospect also grooms all other Snapshots in the Backup Set that require grooming based on the grooming policy you set. See "The Options tab" on page 256 for information on grooming policies.

To manually groom a Snapshot:

1. Choose Configure>Backup Sets from the Retrospect navigation bar.

2. Select a disk Backup Set that has grooming enabled.

NOTE: You can click the Options tab in the Backup Set properties window to see if a grooming is selected.

3. Click the Snapshots tab.

If the Snapshot you want to groom is not displayed in the Snapshots list, click Add to retrieve it from the disk.

4. Select a Snapshot to groom and click Forget.

NOTE: Snapshots with the lock icon 🔒 are protected from grooming and cannot be groomed until they are unlocked. They can be forgotten.

5. Click Forget to remove the selected Snapshot from the Backup Set Catalog File.

WARNING: Once you click Forget, Retrospect *will* groom the Snapshot and its associated files. Click Cancel if you do not want to groom the Snapshot.

6. Close the Backup Set properties window.

The grooming dialog displays.

NOTE: If the selected Snapshot was locked, the grooming dialog does not display.

7. Click Now to groom the Backup Set now.

If you want to groom the Backup Set later, click Later. Retrospect automatically grooms the Backup Set during the next grooming session (as determined by the Backup Set's grooming policy).

It is possible to unlock Snapshots that Retrospect is protecting from grooming.

To unlock a Snapshot:

1. Choose Configure>Backup Sets from the Retrospect navigation bar.

2. Select a disk Backup Set that has grooming enabled.

3. Click the Snapshots tab.

4. Right-click a locked Snapshot 🔒 and choose Unlock.

WARNING: The selected Snapshot is now unprotected and may be groomed (i.e., deleted) from the Backup Set.

You can also protect critical backups by locking individual Snapshots, thereby preventing them from being groomed.

To lock a Snapshot:

1. Choose Configure>Backup Sets from the Retrospect navigation bar.

2. Select a disk Backup Set that has grooming enabled.

3. Click the Snapshots tab.

4. Right-click a Snapshot and choose Lock.

The selected Snapshot is now locked and it displays the lock icon 🔒 next to its name. This Snapshot cannot be groomed.

The Sessions tab

The Session tab lists all archive and backup sessions in the Backup Set. You can see a list of the

files backed up in any session by selecting the session and clicking the Browse button.

The Members tab

The Members tab summarizes the media members of a Backup Set and lets you control its media.

NOTE: This tab is not available for file Backup Sets.

If a member of a Backup Set gets lost or damaged, you can designate it as missing. This lets Retrospect know that the files previously saved to that member are no longer available.

- For tape and CD/DVD Backup Sets, select the missing or damaged member, then click Set Missing.
- For disk Backup Sets, select the member, click Properties, then check "This member is lost or damaged".

During the next backup or archive operation, Retrospect will copy the missing files to a new Backup Set member, ensuring that they are protected.

Tape and disk Backup Sets have an Add button on the Members tab that allows you to configure new Backup Set members in advance. See "Adding Members to Backup Sets" for more information.

For hard disk Backup Sets, you can select any member and choose to skip it. When a member is marked as skipped, Retrospect automatically looks for the next member (or a new member).

To skip a hard disk Backup Set member:

1. Select the member you want to skip, then click Properties.

2. Select the "Skip this member" checkbox.
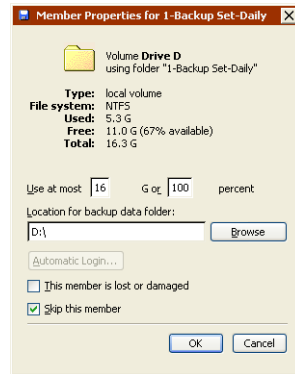
NOTE: If Retrospect uses up all the available space on the disk (or it experiences problems backing up to the disk) it automatically selects this checkbox. You can change the amount of usable memory (if any is available) and deselect the checkbox and Retrospect will try to use this member again.

The Binding tab

The Binding tab is only available for tape Backup Sets and if you have a license for Advanced Tape Support.

When using multiple tape drives with Retrospect, you may want to "bind" a Backup Set to a specific drive. For example, if you have two tape drives, a faster drive and a slower drive, you may want to bind the Backup Set for your client computers to the slow drive, and the Backup Set for the local server to the fast drive. That way the networking speed and drive speed will be more in sync and the tape drives will have to spend less time repositioning the heads.

By default, Retrospect allows Backup Sets to use any available tape drive:

To bind a tape drive:

1. Click the "Selected tape drives" radio button.

2. Select one or more of the tape drives.

NOTE: You can also remove a binding by selecting "Any tape drive".

3. Close the Properties window.

For more information on binding, see "Binding Tape Backup Sets to Tape Drives" on page 163.

Adding Members to Backup Sets

To save time and prevent unattended backups from stopping when media fills up, you can pre-define Backup Set members for tape and disk Backup Sets.

The process for each type of Backup Set varies slightly:

- Adding a Disk to a Backup Set
- Adding Tapes to a Backup Set

Adding a Disk to a Backup Set

You can prepare disks for use ahead of time by adding them as members of a Backup Set. When Retrospect is executing a script unattended and requires additional storage space, it will automatically use the disks you added as members.

To add disk members:

1. Click Configure>Backup Sets.

2. Select a disk Backup Set and click Properties.

3. Click the Members tab.

4. Click Add.
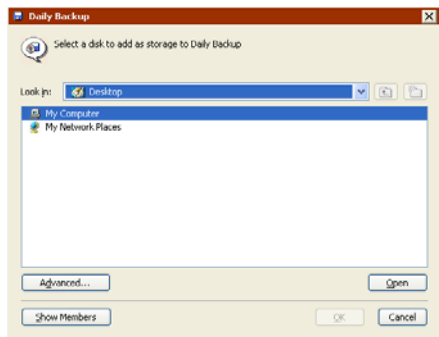
5. Browse to the disk you want to add, select it, and click OK.

For hard disks, a window that appears summarizes information about the disk you are adding and lets you specify how much of the storage space to dedicate to the Backup Set.

6. Click the Advanced button, to specify additional options.

- A location for the backup data folder. If you don't specify a location, the folder is automatically saved on the root level of the disk.
- A password for a network volume so Retrospect can automatically log in during unattended backups.
- With non-system local volumes, you can also have Retrospect erase and rename the disk.

7. Click OK to add the disk.

Adding Tapes to a Backup Set

It is a good idea to prepare tapes for use ahead of time by adding them as members of a Backup Set. When Retrospect is executing a script unattended and requires additional storage space, it will automatically use the tapes you added as members.

To add tape members:

1. Click Configure>Backup Sets.

2. Select a tape Backup Set and click Properties.

3. Click the Members tab.
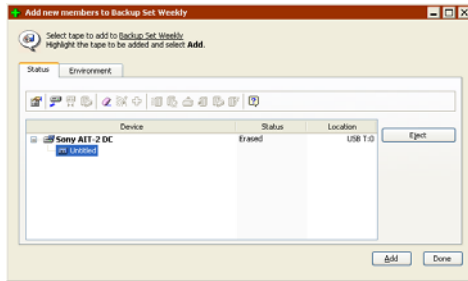
4. Click Add.

5. Select a tape to add to the Backup Set and click Add.

If you have a tape library, you can select multiple tapes to add at one time.

NOTE: Retrospect will not add tapes that already belong to an existing Backup Set. It will add blank, erased, or content unrecognized tapes.

6. Click Done, then close the tape Backup Set Properties window when you're done adding members.

NOTE: You can also add members to a tape backup Set from the Storage Devices window. See "Preparing Tapes for Use" on page 44.

MAINTAINING SCRIPTS

This section provides instructions for various tasks you may need to perform in maintaining the scripts you have created. Maintenance tasks include:

- Checking Scripts
- Modifying Script Settings
- Duplicating, Renaming, or Deleting a Script
- Viewing Scheduled Scripts
- Skipping Script Execution

Checking Scripts

Before exiting Retrospect to run a script unattended, it is a good idea to confirm the script is valid. You can also make sure the required media is available in the backup device.

To check a script

1. From the navigation bar, click Automate> Validate Scripts.

The Script Selection window displays a list of scripts.
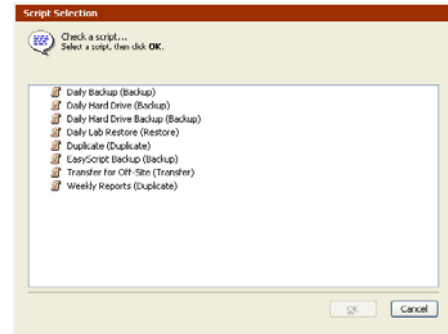
2. Select the script to test and click OK.

Retrospect checks the script definition to make sure that a Source and Destination have been properly defined. A message informs you if the script is missing necessary information. Click Edit to modify the script.

If the script is complete, a message appears telling you the script is ready.
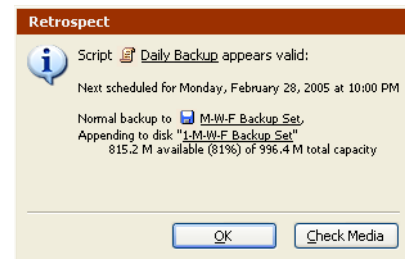
NOTE: The information in this window depends on the type of Backup Set and the media currently loaded in the backup device.

3. Click OK to close the window, or click Check Media to have Retrospect check whether the required Backup Set member is available.

NOTE: When you exit Retrospect, it automatically prompts you to check media for the next scheduled valid script.

Modifying Script Settings

At any time, you can modify the settings you specified when creating a script—you can choose different source volumes or destination Backup Sets, change the file selection criteria, the options, or the schedule. You modify scripts from the script summary window.
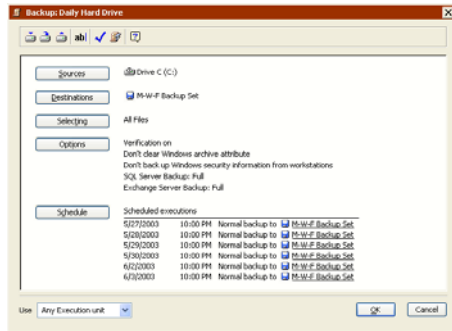
To modify script settings:

1. From the navigation menu, click Automate> Manage Scripts.

2. Select the script to modify and click Edit.

3. Modifying the script is the same as creating it. See Chapter 5 • Automated Operations.

4. Click the Save icon in the toolbar to save the modified script.

Duplicating, Renaming, or Deleting a Script

You can base a new script on an existing one by duplicating a script and then modifying the settings of the duplicate. Scripts can also be renamed or permanently deleted.

To duplicate, rename, or delete a script

1. Click Automate from the navigation bar, then click Manage Scripts to display the list of scripts.

2. Select the script to duplicate, rename or delete.

3. To duplicate the script, click Duplicate from the toolbar.

Enter a name for the new script and click New.

4. To rename the script, click Rename from the toolbar.

Enter a new name for the script and click OK.

5. To delete a script, click Delete from the toolbar.

Click OK to confirm deletion. The script is removed from the list and its scheduled executions are eliminated.

TIP: If you do not want to receive a confirmation message when you delete or duplicate scripts, press and hold the Shift key as you issue these commands.

Viewing Scheduled Scripts

Retrospect maintains a list of upcoming scripts. You can view this list to see which scripts are scheduled to run and when. You can also modify the execution schedule by deleting scheduled events or by editing a script and changing its schedule.

Click Activity Monitor>Scheduled, to view the execution schedule for all scheduled scripts.

NOTE: To view scheduled Proactive Scripts, click the Proactive tab in the Activity Monitor.
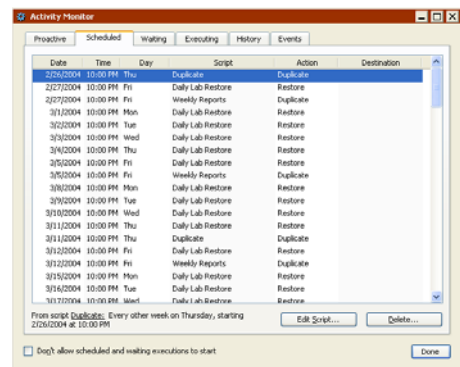
The Scheduled pane displays the date, time, and day of the week that upcoming scripts are scheduled to run. It also lists the script name, backup action, and destination.

Deleting a Scheduled Event

To delete a scheduled event and all prior events for the same script, click the event to select it then click Delete. Click OK to confirm deletion. The event and all prior events for the same script are removed.

Editing Scheduled Scripts

To edit the script associated with an event listed in this window, click the event to select it then click Edit Script. The script summary window appears, and you can click the Schedule button to modify the schedule.

For details on modifying schedules, see "Scheduling Scripts" on page 134.

Skipping Script Execution

If you do not want a script to run for a period of time, you can turn the script schedule off and specify when to turn it on again. This is useful, for example, if your office closes a week for holidays and nobody will be there to change media in the backup device.

To skip script execution:

1. Click Automate>Manage Scripts to display the list of scripts.

2. Select a script then click Edit.

The script summary window appears.

3. Click Schedule.

Retrospect lists the currently scheduled dates and times for this script.
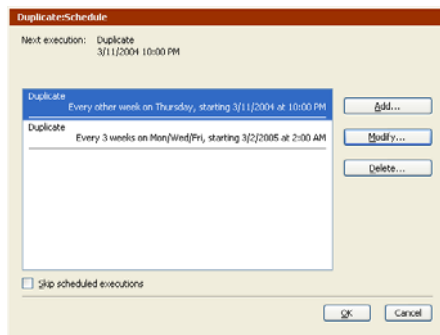
4. Click the Skip scheduled execution checkbox at the bottom of the window.

A date and time field appears at the bottom of the window.

5. Set the date and time at which the script is to again be allowed to execute, then click OK.

Retrospect ignores execution events prior to the date.

NOTE: When multiple schedulers are shown in the script schedule window, the selected scheduler is not the only one skipped by this feature. It skips *all* the scheduled executions for this script.

RETROSPECT PREFERENCES

You can adjust Retrospect preferences to modify the application's behavior to best meet your needs. Retrospect preferences are global, that is, they affect all operations performed by Retrospect.

To access Retrospect preferences, click Configure from the navigation bar, then click the Preferences button. The Preferences window displays.
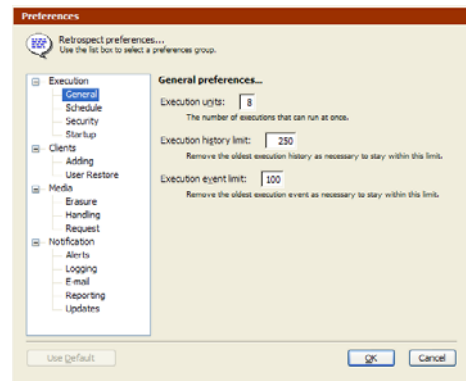
The list box on the left contains the category options. The options for the selected category

appear on the right. Set the options, then click OK to save your selections.

If you change the default setting for an option, the category name will appear in bold in the list box. To restore the default settings, select the category name and click Use Default.
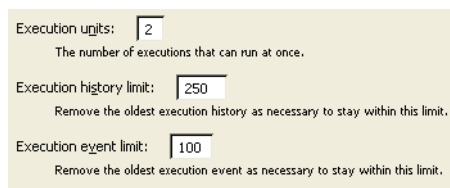
Execution Preferences

The Execution preferences control Retrospect's execution units, look ahead time, and password protection, among other things.

There are four categories of Execution preferences:

- General Preferences
- Schedule Preferences
- Security Preferences
- Startup Preferences

General Preferences

Depending on which edition of Retrospect you have and which add-ons are licensed, you can: change configuration settings during execution; execute independent operations in parallel; handle resource conflicts (including serializing conflicting executions); have the Proactive Backup system kick off multiple executions; and use multiple drives in a tape library simultaneously. See "Multiple Executions" on page 161 for more information.

NOTE: Retrospect Professional does not support multiple concurrent executions.

Execution units lets you specify the maximum number of concurrent operations Retrospect can run. If your edition of Retrospect supports multiple execution units, this option is
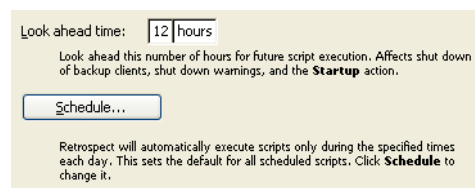
automatically set to the optimal number based on the backup computer's total amount of memory.

NOTE: The software allows up to 8 concurrent executions, provided the computer has enough memory and backup devices to support such a configuration.

Execution history limit specifies the maximum number of operations to save in the Activity Monitor's History tab. Once this maximum is reached, Retrospect replaces the oldest operations with newer ones to stay within the limit. See "History Tab" on page 157 for more information.

Execution event limit specifies the maximum number of events to save in the Activity Monitor's Events tab. Once this maximum is reached, Retrospect replaces the oldest events with newer ones to stay within the limit. See "Events Tab" on page 158 for more information.

Schedule Preferences

Look ahead time: *n* **hours** defines the number of hours Retrospect looks ahead for scheduled script executions. This affects what happens when you begin to shut down the backup computer or a Macintosh client, and what Retrospect does when it completes an unattended operation. The default preference is twelve hours.

For more information, see "Alerts Preferences" on page 270, "Macintosh Client Options" on page 249, and "Startup Preferences" on page 266.

Schedule lets you define a window during which scripts are allowed to execute. This preference affects all scripts, except Proactive Client Backup scripts, but it can be modified for individual scripts. The default window during which scripts are allowed to run is twenty-four hours a day, seven days a week.

To customize the schedule:

1. Click Schedule.

The Weekly Schedule window displays.
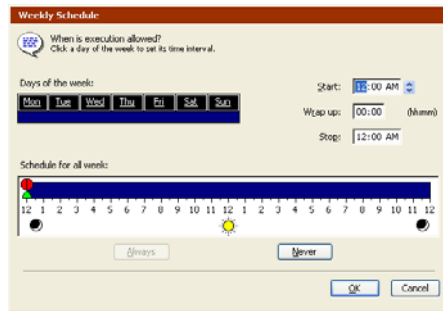
2. To select a day of the week, click it. Click and drag to select contiguous days of the week. Use the Shift or Control key and click or drag to select days without deselecting the previous selection.

To change a time, click on it and type or use the control.

- **Start** is the earliest time at which scheduled executions may begin.
- **Wrap Up** is the period of time (in hours and minutes) before the stop time, during which Retrospect should complete the current operation but not begin new operations.
- **Stop** is the time at which Retrospect absolutely must halt scripted operations (until the next start time).

NOTE: You can also set times by dragging the icons on the hourly schedule bar, but you should first experiment by typing the times to see how these controls work.

When a time is changed, the hourly schedule bar changes accordingly to graphically represent the start, wrap-up, and stop times.
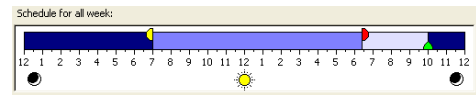
Each selected day has a scaled-down hourly schedule bar, though it does not have controls.

The Always and Never buttons set the daily operating time to twenty-four hours and none, respectively.

3. Click OK when done.

Security Preferences
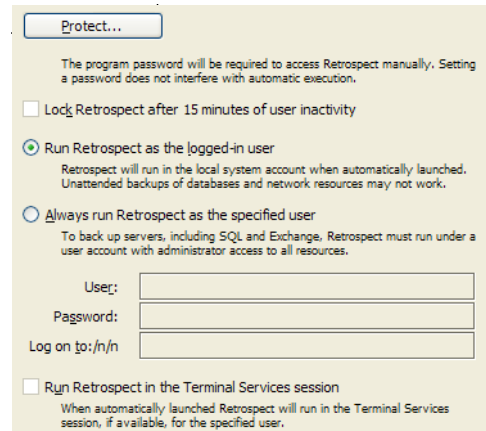
Protect allows you to specify a password that must be entered to start Retrospect manually, though it does not interfere with automatic script execution. If a user enters three incorrect passwords an error is recorded in the Operations Log. By default, there is no password protection.

When protection is added Retrospect enables the Lock Application item in the File menu. Choose this item to force Retrospect into locked, unattended mode to prevent someone

from interrupting executions. Click the mouse or press a key to enter the password and unlock the application.

In order to access the administrator view of the User Initiated Restore (UIR) web page, Retrospect *must* be password protected. The same password that protects Retrospect can be used to access administrator UIR. See "User Initiated Restore" on page 191 for more information about UIR.

Lock Retrospect after 15 minutes of user inactivity allows you to specify that Retrospect should automatically lock after 15 minutes. When Retrospect is locked, you will need to enter the password to unlock it again. You can only select this preference when Retrospect is password-protected.

Unprotect lets you enter the password and remove the protection from the Retrospect application. Unprotect appears only when Retrospect already has a password.

Run Retrospect as... lets you choose the user account under which Retrospect runs.

Run Retrospect as the logged-in user, provides access to only those resources available to that user. In addition, when you select this option and Retrospect is launched automatically to run a script, it will run under the local system account and only have access to resources available to that account.

What this means is that if you choose to run Retrospect as the logged-in user, you may not have access to SQL or Exchange servers or network volumes.

Always run Retrospect as the specified user, allows you to specify a user account that Retrospect will run under whether it is manually or automatically launched.

If you plan to back up SQL or Exchange servers, or need access to network volumes, you should create an account that has administrator access to all of those resources and enter that information here.

For SQL and Exchange, make sure the account has the necessary privileges to access all the database servers you want to back up. See Appendix A: SQL Server Agent and Appendix B: Exchange Server Agent for more information.

For network volumes make sure the account has the necessary privileges to access any volume you want to use as a source, destination, or location for saving Catalog Files.

TIP: Enter either your domain or local computer name into the "Log on to" field, depending on your situation.

Run Retrospect in the Terminal Services session lets you choose to run Retrospect in the Terminal Services session (if available) when the application is automatically launched. See "Terminal Services and Remote Desktop" on page 276.

Startup Preferences

Enable Retrospect Launcher service registers the launcher application as a service so it is always running. This allows the auto-launch preference described below, the alert preferences described in "Alerts Preferences" on page

270, and the reporting preference described in "Reporting Preferences" on page 272.

Automatically launch Retrospect automatically starts Retrospect when a scheduled script is waiting to execute. By default, this preference is turned on.

NOTE: If the Stop all execution activity button on the Retrospect toolbar is selected, this preference is turned off and disabled. It is enabled and turned on again when the Stop button is deselected. See "Stop Button" on page 152 for more information.

Stay in Retrospect, Exit, Log off, Restart, and Shut down determine what Retrospect does when a script is completed and no additional scripts are scheduled in the specified look ahead time. (See "Schedule Preferences" on page 264.) By default, this preference is set to Exit.

Show taskbar icon tells Retrospect whether or not to display the Retrospect icon in the Windows taskbar's system tray. This preference is on by default. See "The System Tray Icon" on page 19 for more information.

Clients Preferences

The Clients preferences control the creation of private and public keys, automatically adding clients, and User Initiated Restore.

NOTE: These preferences are not available for Retrospect Professional.

There are two categories of Clients preferences:

• Adding Preferences
• User Restore Preferences

Adding Preferences
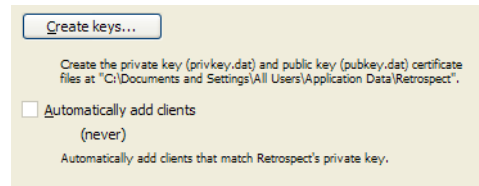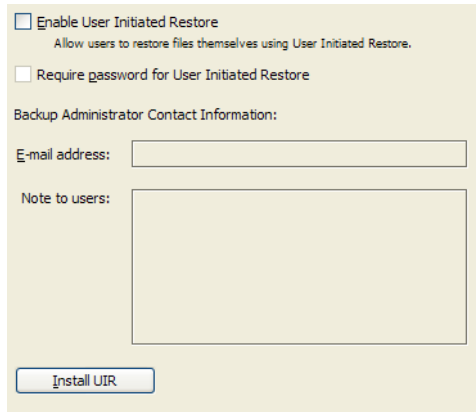
Create keys creates a private key certificate (privkey.dat) and a public key certificate (pubkey.dat) at "C:\Documents and Settings\All Users\Application Data\Retrospect". These keys can be used to add multiple Retrospect Client for Windows users to Retrospect's Backup Clients Database at once. See "Adding Clients" on page 171 for more information.

Automatically add clients enables Retrospect to automatically discover Retrospect Client for Windows users that were installed with the public certificate key and add them to the Backup Clients Database. Select the check box, then specify how frequently (in days or hours) Retrospect should look for new clients. When you click OK to accept your selections, Retrospect immediately looks for new clients and then waits the specified period of time before checking again.

By default, Retrospect adds the clients it finds to the "Automatically Added Clients" folder in the Backup Clients container. If you enable this preference and choose the "Automatically Added Clients" folder as the source for a scripted backup, Retrospect will automatically add new clients to the folder and back them up without requiring any action from the backup administrator.

NOTE: This preference only adds clients that Retrospect can discover using the multicast or subnet broadcast methods. See "Access Methods" on page 179 for more information on these methods.

User Restore Preferences

Enable User Initiated Restore allows users to access the User Initiated Restore web page and restore their own files. User Initiated Restore (UIR) is an add-on product and requires a license code. See "User Initiated Restore" on page 191 for more about setting up and using UIR.

Require password for User Initiated Restore prevents Retrospect Client users from accessing the User Initiated Restore web page without entering a password. If you enable this preference, you will have to enter a password for each client on the Tools tab of its Client Properties window. See "Tools Tab" on page 174 for more information. You can also select multiple clients in the Backup Clients Database then right-click the selection and choose Set User Restore Password. In this case, all selected clients will have the *same* UIR password.

NOTE: If you require a UIR password, you must update all your Windows, Linux, and Mac OS X clients to the latest Retrospect Client software. Although UIR *is* supported with older versions of Retrospect Client for Windows, Linux, and Mac OS X, these clients do not support UIR passwords and they cannot use UIR if a password is required.

Backup Administrator Contact Information allows you to enter the backup administrator's

e-mail address and notes to users. This information will be available to Retrospect Client users from the UIR web page.

Install UIR launches the User Initiated Restore Setup Wizard, which guides you through the process of installing UIR. See "Installing User Initiated Restore" on page 192 for more information.
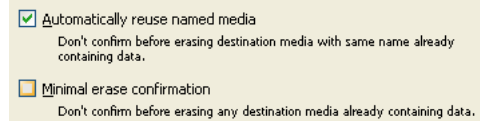
Media Preferences

The Media preferences control how Retrospect works with storage media including media requests, erasing media, retensioning tapes and more.

There are four categories of Media preferences:

- Erasure Preference
- Handling Preferences
- Request Preferences
- Verification Preferences

Erasure Preference

These options only affect media that already have data on them.

Automatically reuse named media When this preference is selected, Retrospect automatically erases destination media with the same name when the media already contains data. By default this option is selected.

For example, if this option is selected and you do a Recycle backup to a tape Backup Set member named "1-Backup Set A", and a member with that name is loaded in your tape drive, Retrospect will automatically erase and reuse the tape. In this case, Retrospect does not display a warning dialog asking if you really want to erase the tape.

Minimal erase confirmation When this preference is selected Retrospect skips the confirmation message that normally appears when you proceed with a backup operation and Retrospect needs to erase the media. By default, this preference is turned off.

For example, let's say you do a Normal backup to a tape member Backup Set named "1-Backup Set A", but the only member loaded in your tape drive has a different name. Retrospect displays the media request window in which you can select the currently loaded tape. If the minimal erase option is checked and you select the tape and click Proceed, Retrospect will erase and use the tape. If the minimal erase option is unchecked, Retrospect displays a warning dialog asking if you really want to erase the tape.

Handling Preferences

Retension tapes winds a tape forward to the end and back to even out the tension and alignment. (This applies only to some drives.) By default, this preference is turned off.

Don't eject removable disks prevents Retrospect from ejecting removable disks when it needs other media in operations. By default, this preference is turned off.

Eject tapes and discs when exiting does so with tape cartridges and CD/DVD discs when

Retrospect exits. By default, this preference is turned off.

Stop Removable Storage Manager causes Retrospect to automatically stop Windows 2000 and XP's Removable Storage service when Retrospect scans the communications bus for devices. With the service stopped, which is the default for this preference, you cannot use the Removable Storage management console to manage tape libraries and other storage devices in conjunction with the operating system's built-in backup utility.

If you need the Removable Storage service intact for managing devices other than those used by Retrospect, you can deselect this preference and configure Removable Storage in order use both simultaneously. See "Using Retrospect and Removable Storage Simultaneously" on page 49.

WARNING: Deselecting this preference may cause problems if you don't also configure Removable Storage.

Use new media automatically after write failure allows Retrospect to continue backup, archive, and transfer operations to a tape library or autoloader, even after a media failure. If this option is selected and Retrospect encounters a media failure, it looks for the next available tape and uses it instead.

TIP: The tape that caused the media failure will appear with a red tape icon in Retrospect's Storage Devices window.

Use ASPI to communicate with devices By default, Retrospect communicates with devices using NT Passthrough. Do not change this preference unless directed to do so by Tqzkq Retrospect Technical Support.

Request Preferences

Media request timeout
    (never)
Limit the time Retrospect waits for media during execution.

Automatic skip to blank media
Use a blank tape/disk/disc when the last member of the Backup Set is not available, even though it's not yet full.

Media request timeout specifies a period of time for Retrospect to wait for media during execution. When the time elapses, the execution stops and Retrospect proceeds according to the next scheduled event. This preference is off by default, so it never times out.

Automatic skip to blank media allows Retrospect to use any available blank tape, disk, or CD/DVD when the current member of the Backup Set is not available; even when the current member is not full. Retrospect performs a Normal backup (i.e., only new and changed files since the last backup) to the blank media, which is added as a member of the destination Backup Set.

By default, this option is not selected and Retrospect always displays a media request when the current member of the Backup Set is not available. See "New Member Backups" on page 25 for information on a related backup action.

WARNING: This preference should not be turned on when you are using WORM tapes. Since WORM tapes cannot be erased or reused, you want to make sure each tape is filled with data before moving to a new tape.

Verification Preferences

Generate MD5 digests during backup operations
MD5 digests enable the Media Verification option and offline verification. Only turn this option off if performance issues are encountered.

Generate MD5 digests during backup operations enables the Media verification option for backup and archive operations, as well as for offline verification. See "Scripted Verification"

on page 132, "Backup Execution Options" on page 237, and "Verifying Backup Set Media" on page 305 for more information.

NOTE: Disable this preference *only* if you experience significant performance issues during backups.

Notification Preferences

The Notification preferences control the types of alerts Retrospect displays, the size of the log, and e-mail notifications.

There are three categories of Notification preferences:

• Alerts Preferences
• Logging Preferences
• E-mail Preferences
• Reporting Preferences
• Updates Preferences

Alerts Preferences
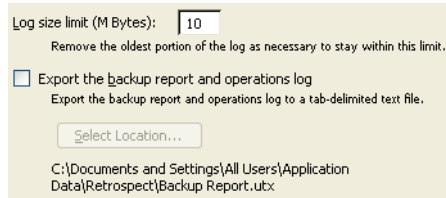
Check validity of next script
Display information on the next scheduled script when exiting.

Notify for failures and media
Notify for serious failures after automatic execution and when media will be needed in the future.

Report HP Compaq SMART hard drive errors
Present a backup wizard when HP Compaq SMART hard drive errors are reported.

Check validity of next script does so when you quit Retrospect. It automatically verifies and displays information about the next script scheduled to execute. By default, this preference is turned on.

Notify for failures and media displays an alert message if errors occur during the automatic execution of a script. It also displays an alert message when media will be needed in the future. By default, this preference is turned on. This option is only available if the Enable Retrospect Launcher service unattended execution preference (see page 266) is on.

Report HP Compaq SMART hard drive errors opens Retrospect and starts a backup wizard when Retrospect learns of errors on HP Compaq SMART hard drive volumes. By default, this preference is turned on.

Logging Preferences

Log size limit (M Bytes):   `10`
    Remove the oldest portion of the log as necessary to stay within this limit.
☐ Export the backup report and operations log
    Export the backup report and operations log to a tab-delimited text file.

    [Select Location...]
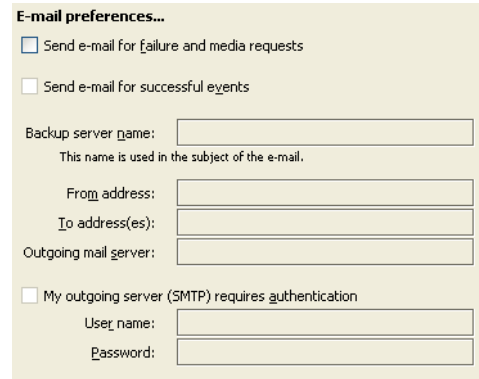
    C:\Documents and Settings\All Users\Application
    Data\Retrospect\Backup Report.utx

Log size limit (M Bytes) maintains the Operations Log size within the limit you set in the field provided. You can set the limit anywhere between 1MB and 100MB. When the log reaches the limit, the oldest portion of the log is deleted to keep its size within the limit. The default size is 10 MB.

Export the backup report andoperations log produces or updates a backup report file (Backup Report.utx) and an operations log file (operations_log.utx) after each execution. The files are stored in alocation you specify with the Select Location button.

See "Printing or Exporting the Backup Report" on page 231 and "Printing or Exporting the Log" on page 232 for moreinformation on how to export these files manually.

E-mail Preferences

E-mail preferences...
☐ Send e-mail for failure and media requests

☐ Send e-mail for successful events

Backup server name:
    This name is used in the subject of the e-mail.

    From address:
    To address(es):
Outgoing mail server:

☐ My outgoing server (SMTP) requires authentication
    User name:
    Password:

Send e-mail for failure and media requests, when selected, enables Retrospect to send e-mail to one or more recipients after failed operations or media requests.

Send e-mail for successful events, when selected, enables Retrospect to send e-mail to one or more recipients after successful operations.

NOTE: This option isonly available if the Send e-mail for failure and media requests check box is selected.

If e-mail notifications are enabled, Retrospect automatically enters the host computer name in the Backup server name field. You can enter a different name. This information is included in the subject field of e-mail notifications.

Enter the sending account in the From address field and enter one or more recipient accounts (separated by semicolons) in the To address field. Enter the mail server DNS name (e.g., mail.tqzkq.com) in the Outgoing mail server field.

If your mail server requires SMTP authentication, select that check box and enter the user name and password.

Reporting Preferences

Reporting preferences...

☐ Enable notification for external applications

   Allows external applications such as NetWorker Management Console to connect to Retrospect and display Retrospect events.
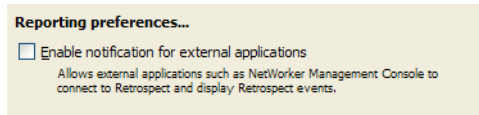
Enable notification for external applications allows applications, such as EMC Legato Net-Worker Management Console (NMC) to connect to Retrospect and display Retrospect events. This allows a backup administrator to monitor both NetWorker and Retrospect back-up servers from a single console.

NOTE: Retrospect can only notify external applications about events if the Retrospect Launcher service is enabled. See "Startup Preferences" on page 266.

For more information on events, see "Events Tab" on page 158. For more information on monitoring and managing Retrospect backup servers from the NetWorker Management Console, see the NMC documentation.

NOTE: This preference is not available for Retrospect Professional.

Updates Preferences

Updates preferences...

☑ Automatically check for available updates

   Automatically checks the Retrospect web site for available updates to this version of Retrospect.

☐ Use a proxy server to connect to the internet

   Proxy server: [   ]
   Port: [   ]
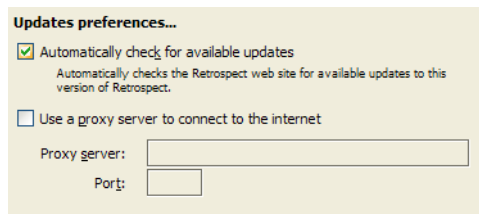
Automatically check for available updates is selected by default. When selected, Retrospect checks for free updates to your current version of Retrospect on a regular basis. If Retrospect finds an update, it displays a list of all available updates, which you can download and install. Retrospect Updates are free downloads that provide additional device support or address issues with your current version of Retrospect. Regardless of whether or not this preference is not

enabled, you can always manually search for updates by choosing Retrospect Updates from the Help menu. See "Manually Checking for Retrospect Updates" on page 16 for more information.

NOTE: Retrospect cannot check for updates if the backup computer does not have an Internet connection.

Use a proxy server to connect to the internet lets you specify proxy server information. A proxy server is an intermediary between an internal network and the Internet. If you are not sure if you use a proxy server or not, contact your network administrator. If you use a proxy server to connect to the Internet, select the check box and enter the proxy server information and port number here, for example, cache.satchmo.com, port 8080.

Sounds

After installing Retrospect, the backup computer's Windows Sounds control panel includes the Retrospect Attention Sound and Completion Sound. You can assign any available sound to these events.

MOVING RETROSPECT

If you ever decide to switch backup computers, you must do more than just install Retrospect and your backup device on the new machine. You must move some other files to the new backup computer in order to keep Retrospect's preferences, clients, catalogs, scripts, and schedules intact.

To move Retrospect to a new backup computer:

1. Install Retrospect on the new computer.

2. Copy the Catalog Files (with name extensions .rbc and .rbf) from the old backup computer to the new computer.

NOTE: The default location that Catalog Files are saved is ..\My Documents\ Retrospect Catalog Files.

3. Copy the configuration file (Config75.dat) from the old backup computer to the new computer.

NOTE: The configuration file is saved is either in the same folder as the Retrospect application, or in ..\Documents and Settings\All Users\Application Data\Retrospect.

4. Next, you must force Retrospect (on the new backup computer) to recognize the Catalog Files you just moved.

The easiest way to do this is to select all of the catalogs in the Windows Explorer, and drag them onto the Retrospect application icon. Retrospect opens a Backup Set configuration window for each Catalog, causing it to recognize the catalogs.

5. If you want to back up the old computer and/or the new backup computer, you must perform a few extra steps:

- If the new backup computer was previously backed up as a client, that is no longer necessary since its volumes are now local. Forget the client. Edit the sources in any Retrospect scripts which used client volumes from the new computer and add the volumes which are now local.

- If you still want to back up the old backup computer you must install Retrospect client software on that machine to access its volumes with Retrospect from the new backup computer. After installing and configuring the client, add its volumes to your scripts. Click Configure>Volumes and use the Forget command to remove the previously local volumes. Forgetting volumes removes them from the volumes database and any scripts which use them.

CATALOG AND CONFIGURATION BACKUPS

Part of your backup strategy should be to back up the backup computer. The simplest way to do this is to include the computer in your backup scripts. The most important files to back up are Retrospect's backup configuration file (Config75.bak) and your Catalog Files (.rbc files).

You can use the Windows Explorer or Retrospect to back up these files. Periodically copy them to another volume, such as a removable disk or file server, to help you recover from a disaster more quickly. Or, set up a Retrospect duplicate script to automatically copy the files to a folder on another volume. Use the Retrospect Files selector to select appropriate files, and schedule the script to run daily, when your other backups are complete.

If you back up your backup computer to multiple Backup Sets, your catalogs and configuration are automatically covered in case of a disaster. Each Backup Set contains backups of the other Backup Sets' catalogs. Alternatively, if you have several large catalogs, consider backing them up to their own dedicated Backup Set to help recover from a disaster or lost Catalog faster.

Catalog Backups

Catalog files are important adjuncts to Backup Sets, but face the same risks as your files since they often share the same hard disk. If you lose your Catalog Files, Retrospect cannot restore any files until the catalogs are recreated, which can be a lengthy process. For this reason, back up your Catalog Files as well as your regular files.

The default location that Catalog Files are saved is ..\My Documents\ Retrospect Catalog Files.

TIP: Create a separate Backup Set for just Catalog Files and back them up on a regular

basis. This will save time when you need to restore files.

Configuration Backups

Retrospect's configuration file contains your client database, scripts, schedules, preferences, custom selectors, and other important information. Retrospect uses the configuration file, named Config75.dat, located in the folder in which the Retrospect application resides or at the path:

..\Documents and Settings\All Users\ Application Data\Retrospect\

Each time you exit Retrospect, it automatically saves a backup copy of Config75.dat in a file named Config75.bak. You should back up this file regularly. If your active configuration file (Config75.dat) is ever lost or becomes corrupt, delete it then open Retrospect, which creates a new Config75.dat from the Config75.bak.

WORKING WITH FILE SERVERS

Retrospect is compatible with Windows 2000 Server and Advanced Server, Windows Server 2003, Windows Small Business Server 2000, Windows NT 4.0 Server, and Apple's Mac OS X servers. Retrospect can back up files from any server to which the backup computer has access via Windows Explorer.

NOTE: Retrospect does not support clusters or SharePoints.

Backing Up a Server to Move its Contents

If you are going to back up a server to move its contents (for example, you have a more powerful computer to be the new server) you should make two separate verified backups. Through verification, which is on by default, ensures the integrity of the data; having two backups will not leave you stranded if one fails for some reason.

Backing Up DHCP Server and WINS Server Information

Retrospect does not back up certain active DHCP and WINS server files. However, the operating system can maintain its own backups, which you can back up from Retrospect.

The DHCP server copies its files to a folder named "backup" in the "dhcp" folder, once an hour. The WINS server, by default, does not make copies of its needed files, but you can make it do so.

If you need to back up a Windows server running WINS, take the steps described below to make these files available for Retrospect backups.

To prepare the WINS server for backup:

1. For Windows NT, use the WINS Manager and go to Server>Configuration>Advanced.

For Windows 2000, use WINS and go to Action>Properties.

2. Set the backup database path to %SystemRoot%\configbk\ then exit WINS or WINS Manager.

If the folder you specified does not exist, it will be created automatically.

After you take these steps, the WINS files will be copied to the backup folder every three hours.

Backing Up the Configurations

It is important to make sure that your backups include the DHCP/WINS backup database paths (the backup and configbk folders).

TIP: The All Files and OS Folder selectors ensure the files will be included in backups.

Restoring the DHCP and WINS Databases

To restore the DHCP and WINS databases, follow the steps under "Restoring from a Full Backup" on page 207. After completing the

steps, DHCP or WINS server information is restored.

Microsoft Exchange Server

The Retrospect Exchange Server Agent provides specialized support for optimally backing up Microsoft Exchange 2003, Exchange 2000, and Exchange 5.5 servers and mailboxes. It is an add-on product that must be purchased separately and requires a license code.

The Exchange Server Agent uses Microsoft APIs to effortlessly and automatically protect a Microsoft Exchange server that runs continuously and cannot be stopped for backups.

See Appendix B: Exchange Server Agent for more information.

Microsoft SQL Server

The Retrospect SQL Agent provides specialized support for optimally backing up Microsoft SQL 7.0 and Microsoft SQL 2000 servers. It is an add-on product that must be purchased separately and requires a license code.

The Retrospect SQL Agent uses Microsoft APIs to effortlessly and automatically protect a Microsoft SQL server that runs continuously and cannot be stopped for backups.

See Appendix A: SQL Server Agent for more information.

Backing Up Mac OS File Servers

This section describes how to use Retrospect to back up volumes shared by Mac OS file sharing. These operations require special procedures to ensure access privileges are intact after the volume is restored.

Restoring servers is described in "Restoring Mac OS File Servers" on page 215.

Shared volumes maintain access privileges that determine which users and groups of users can see and change files and folders. These privileg-

es are active only when the server is running and the volume is shared.

To retain access privileges for a server, file sharing must be on during the backup. During a subsequent restore operation, Retrospect reassigns privileges to the same users and groups that were active during the backup. Otherwise, any privileges for the restored and retrieved folders revert to the volume owner or server administrator.

WORKING WITH OPEN FILES

With Open File Backup, you can back up, duplicate, and archive files, even if they are in use. Open File Backup can protect multi-volume datasets, enabling you to copy related open files across multiple volumes.

Requirements for Open File Backup

- Retrospect Disk-to-Disk, Small Business Server, Single-Server, or Multi-Server
- License code for Open File Backup. Open File Backup must be purchased separately. Click Configure>Licenses to view your current licenses or purchase new ones.
- The volume being backed up must be running Windows NT 4.0 Server or Workstation with Service Pack 6; Windows 2000 Professional, Server, or Advanced Server with Service Pack 2; or Windows XP. To back up open files on a Windows XP computer, it must have an NTFS volume.
- If the volume being backed up is a client, it must be running Retrospect Client 6.0 or greater.

NOTE: If you have Retrospect Professional, you can use Open File Backup, as long as the backup computer is running Windows XP and it has an NTFS volume. You do *not* need a license code to use Open File Backup in this case.

Options

Retrospect has a number of options that are specific to Open File Backup. See "Windows Open Files Options" on page 247 for more information.

Backing Up SQL and Exchange Servers

You *can* back up SQL and Exchange servers using Open File Backup, however, the Retrospect SQL Agent and Retrospect Exchange Agent provide specialized support for optimally backing up these servers. Tqzkq recommends using the agents instead of Open File Backup for SQL and Exchange servers.

See Appendix A: SQL Server Agent and Appendix B: Exchange Server Agent for more information.

Open File Backup Tips

If you plan to use Open File Backup, Tqzkq strongly recommends that you follow the tips below.

Perform thorough testing of Open File Backup before using it on production systems. Every environment is unique and it is important to ensure your data is backed up accurately and completely. Do a complete backup and restore of volumes containing open files. Check for data integrity and application functionality on the restored volume.

Optimize your environment, scheduling, and Open Files options to maximize disk inactivity. Open File backup requires a period of inactivity on the source volume's disk (disk inactivity threshold) in order to accurately copy open files.

To avoid error messages:

- Schedule scripts that use Open File Backup during off-peak hours.

- Experiment with the Disk inactivity threshold and Retry timeout options to determine optimal values. A lower disk inactivity threshold increases the chances that it will be met, but also increases the possibility of data inconsistency. A higher disk inactivity threshold decreases the chances that it will be met, but also decreases the possibility of data inconsistency.

- During Open File Backup, disable or stop applications on the source volume's disk that could increase disk activity, e.g. anti-virus software, disk defragmentation software, etc.

- If the Open File Backup operation includes multiple volumes, but none of the open file data spans multiple volumes, make sure the Protect Multi-Volume Datasets option is off.

NOTE: If you have other applications with open file backup capabilities, you may experience problems with Retrospect's Open File Backup.

TERMINAL SERVICES AND REMOTE DESKTOP

Microsoft Terminal Services allows a user to remotely control an application running on a remote server by transmitting only keyboard, mouse, and display information over the network. Each Terminal Services user connects to the server by establishing an individual session, which is managed by the server, independent of other user sessions. The following best practices describe how to use Terminal Services to administer Retrospect when it is running on a remote server.

Connecting to and Configuring the Server

The Windows server must be configured properly to ensure that Retrospect can run under the correct user account.

To connect to a Windows server via Remote Desktop (the Terminal Services client):

1. Click Start, point to All Programs, point to Accessories, point to Communications, and then click Remote Desktop Connection.

2. Type in the IP address of the server and click the Connect button.

To connect to a Windows Storage Server 2003–based server via a Web browser:

1. Launch Internet Explorer.

2. Type in the IP address of the server followed by :8098 to connect to the server.

For example: https://192.168.1.1:8098

3. Click the Maintenance tab.

4. Click the Remote Desktop icon.

Creating or Modifying a User Account to Run Retrospect

To separate your backup tasks from your default Administrator account, create a Backup Administrator account on the server and assign Administrator rights to the account.

To create a Backup Administrator account with Administrator rights:

1. Right-click My Computer and choose Manage.

2. In Computer Management, expand Local Users and Groups and select Users.

3. In the Action menu, select New User…

4. For the User name and Full name, type Backup Administrator.

5. Choose a secure password.

6. Uncheck User must change password at next login.

7. Check Password never expires.

8. Click the Create button.

9. Double-click the newly created user to see its properties.

10. Click the Member Of tab.

11. Click the Add… button.

12. In the Enter the object names to select: field, type Administrators, then click Check Names.

13. Click the Sessions tab.

14. Ensure that the End a disconnected session: option is set to Never.

15. In the Properties window, click Apply and then click OK.

NOTE: If you want to use your Administrator account for backup administration, ensure that you set up your Administrator account with the options defined in the preceding procedure.

After you create a Backup Administrator account, close the remote window to disconnect from the current session or log off from the current account. Then log in using the Backup Administrator account in order to configure the Terminal Services connection properties.

To configure the Terminal Services connection properties:

1. Open the Administrative Tools control panel folder.

2. Launch the Terminal Services Configuration control panel.

3. Highlight Connections in the navigation bar, right-click RDP-TCP and select Properties.

4. Click the Sessions tab.

5. Ensure the Override User Settings option is unchecked.

6. Click Apply and then OK.

Installing and Setting Up Retrospect on the Remote Server

Perform the following procedures to install and set up Retrospect so that you can use it remotely via Terminal Services. Retrospect must always be run under the same specific account (usually the Backup Administrator account discussed in the preceding section) for you to successfully access it remotely. To ensure that Retrospect al-

ways launches under that specific account, you must modify Retrospect's security preferences.

To install Retrospect:

1. Connect to the server using Terminal Services or Remote Desktop.

2. Copy the Retrospect installer to the server.

3. Install Retrospect.

To set up Retrospect:

1. Connect to the server using Terminal Services or Remote Desktop.

2. Log on to the account you want Retrospect to run from.

3. Launch Retrospect.

The first time you start Retrospect, the Getting Started Wizard runs.

4. In the user account screen, select "Always run Retrospect as the specified user" and enter user, password and domain information.

NOTE: A user must have Administrator privileges to all network resources and SQL/Exchange servers that the user plans to access.

5. Click OK.

6. Click Yes to run Retrospect in the Terminal Services session.

7. Finish the Getting Started Wizard.

8. Click Relaunch Now to quit and restart Retrospect.

NOTE: You can change Retrospect's login and Terminal Services preferences later by choosing Configure>Preferences from the Retrospect navigation bar and clicking Security. See "Security Preferences" on page 265.

Keeping Retrospect Running

Logging off from the Terminal Services session causes all running applications to quit, including Retrospect. To ensure that Retrospect continues to run, do not use the log off option in the Start menu to log off from Terminal Servic-

es. Instead, simply close the Terminal Services window.

Closing the window disconnects you from the Terminal Services session, but leaves the session running. Retrospect remains unaffected, and the next time you connect to the remote server via Terminal Services, Retrospect will be running.

CHAPTER *10*

TOOLS

- **WORKING WITH VOLUMES**

- **BROWSING**

- **USING SELECTORS**

- **MAINTENANCE AND REPAIR**

- **EXTERNAL SCRIPTING**

Retrospect has a number of features that go above and beyond the basics required for backup and restore operations. Your knowledge of these features is not essential to use Retrospect, but knowing them allows you to work with the program more quickly and more efficiently.

WORKING WITH VOLUMES

A volume is the operating system's representation of a random-access storage device, such as a hard disk drive or partition, removable disk, or CD/DVD. It can also be a file server on the network. A volume is the basic storage unit containing files and folders. Retrospect uses volumes as sources for backups and other operations and helps keep track of files with volume Snapshots.

If the backup computer or a logged in client has Microsoft SQL Server or Exchange Server installed, they will also appear in Retrospect's volume list windows. If Exchange Server is installed an additional container, Exchange Mailboxes, will also appear.

NOTE: In order to back up and restore SQL and Exchange databases and mailboxes, you need Retrospect's SQL Server Agent and Exchange Agent. See Appendix A: SQL Server Agent for more information on working with SQL servers. See Appendix B: Exchange Server Agent for more information on working with Exchange servers and mailboxes.

Volume List Windows

Retrospect has two volume list windows. Many Retrospect operations use a volume selection window for you to select one or more volumes for the operation at hand.
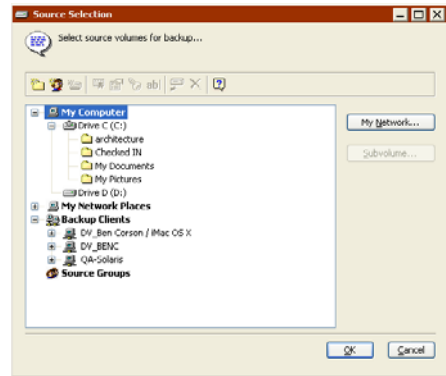
The volume selection window for an immediate backup.

A similar window, the Volumes Database window, can be used to manage volumes. The Volumes Database window has some additional features that are not available from the volume selection windows. For example, the Volumes Database window's list is organized for and includes controls for more involved navigation and selection of the listed volumes.
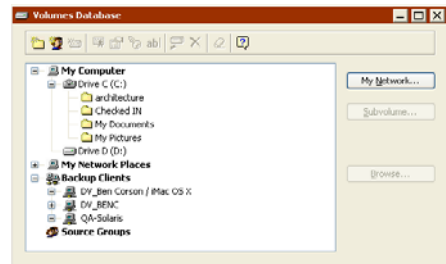
The volumes database window.

Using either window is fairly straightforward; you click on the volumes you want, then click a button or toolbar icon to proceed or act on the selected volume. (You can also right-click to use a contextual menu.)

To practice the techniques described here, open the Volumes Database window by clicking Configure>Volumes.

The volumes listed in the scroll box are organized in an outline format similar to that of Windows Explorer.

Displaying Volumes

In a volume list window, the + and – icons on the left work just like those in the Windows Explorer. Click on a + icon to show the contents of its container (see page 281) or folder (see page 283). Click on a – icon to hide the contents of its container or folder. A volume does not have this control unless it has one or more defined Subvolumes.

Selecting Volumes

In a volume list window, you click on a volume to select it. This deselects any other selected volumes.

Press and hold the Control key and click a volume to select it without deselecting any currently selected volumes. You can make a multiple non-contiguous or contiguous selection this way.

Press and hold the Shift key and click a volume to select all volumes listed from the current selection to the Shift-clicked volume. This is called a contiguous multiple selection.

Some operations do not allow multiple selections. (For example, you cannot restore to multiple volumes.)

Following are examples of these selection methods.

Original selection	After clicking on Iago
Desdemona (C:)	Desdemona (C:)
Iago (D:)	**Iago (D:)**
Othello (E:)	Othello (E:)
Cassio (F:)	Cassio (F:)

After Control-clicking on Iago	After Shift-clicking on Iago
Desdemona (C:)	Desdemona (C:)
Iago (D:)	**Iago (D:)**
Othello (E:)	**Othello (E:)**
Cassio (F:)	**Cassio (F:)**

These methods of making individual and multiple selections work throughout Retrospect, not just in the volume list.

Containers

In a volume list, volumes, clients, and groups are organized under the containers My Computer, My Network Places, Backup Clients, and Source Groups.

Selecting one of these top-level containers selects everything in that container. For example, you could back up every hard disk and removable disk attached to the backup computer, and every client logged into Retrospect, simply by selecting the My Computer and Backup Clients containers as sources.

My Computer

The My Computer container holds local drive volumes. This includes the internal hard disk, any inserted removable disk, and external drives. It does not include mapped network drives or network volumes. The My Computer container also includes local SQL and Exchange databases and Exchange mailboxes.

When you select the My Computer container itself, you are instructing Retrospect to select all volumes in that container on the backup computer, except for floppy disks and CD-ROM discs.

The following example of a My Computer container selection shows the volumes to which it resolves. (For example, if the selection were used in a backup operation, the resolved volumes would be backed up.)

Using this selection…	…resolves to these volumes
🖥 My Computer — 💾 Capulet (C:) — 💾 Montague (D:) — 💾 Star-Crossed (E:)	Capulet Montague

My Network Places

The My Network Places container holds only shared volumes you have added to it.

When you select the My Network Places container itself, you are instructing Retrospect to select all shared volumes contained within it.

To add a network volume to the volumes database:

1. Choose Configure>Volumes from the navigation bar.

2. Click the My Network button.

3. Navigate through the network to the volume or folder you want to add.

NOTE: You can also click Advanced to specify a UNC path to the volume you want to add.

4. Select it and click the Add button.

If the server requires it, enter a login and password and click OK.
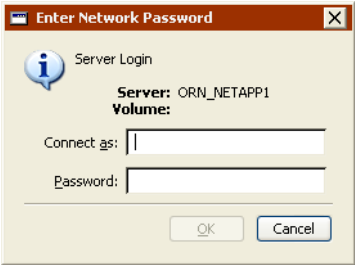
NOTE: If you set Retrospect up to log in as a user with privileges to the network volume, you will not be prompted to log in again. See "Security Preferences" on page 265 for more information.

Backup Clients

The Backup Clients container holds client computers that you have added to it by logging them in for use with Retrospect. Clients themselves contain one or more volumes, which are made available according to how they are configured with the Volumes tab of the client properties window. For details, see Chapter 7 • Networked Clients.

NOTE: Retrospect Client for Windows computers that were automatically added to the Backup Clients Database using the public key/private key method are, by default, grouped in a folder called "Automatically Added Clients" in the Backup Clients container. See "Adding Preferences" on page 267 for more information.

When you select the Backup Clients container itself, you are instructing Retrospect to select all clients contained within it.

NOTE: If you have added SQL or Exchange servers as clients, they appear in the Backup Clients container. If you have an Exchange server client, the Exchange Mailboxes container also appears.

Source Groups

The Source Groups container holds volumes grouped together for better organization. Groups, which you define, do not contain the actual volumes themselves, but aliases which are shortcuts to actual volumes (which are in My Computer, My Network Places, or Backup Clients).

For example, you could make an Accounting group containing the volumes from the accounting department. Later when you are creating a backup script, instead of tediously selecting each individual accounting volume, you can

just select the Accounting group and Retrospect knows you mean all of the volumes within that group.

NOTE: Source Groups are not available in volume lists of duplicate and restore operations.

Creating Groups: To create a new group, choose Configure>Volumes from the navigation bar. In the Volumes Database window, click New Group from the toolbar. After you enter its name in the dialog, the new group appears under the Source Groups container. Any items that were highlighted when the group was created will belong to the new group.

Adding Volumes to Groups: You can drag any item from the My Computer, My Network Places, or the Backup Clients container into a group.

TIP: Since Source Groups contain shortcuts to volumes and not the volumes themselves, the same volume can be added to more than one group.

Arranging Group Items: You can drag any item out of one group and into another group. You can drag an item to a different location within its group to rearrange the order of the group.

Removing Groups: You can remove an unwanted group or item by selecting it and clicking Forget from the toolbar or pressing the Delete key.

Folders

You can create folders to help organize the information that appears in the volume list window. For example, while setting up a backup you can select a folder as a backup source and Retrospect will back up all the volumes in the folder.

NOTE: These folders are specific to Retrospect and do not appear outside the program.

Retrospect Client for Windows computers that were automatically added to the Backup Clients Database using the public key/private key method are grouped in a folder called "Automatically Added Clients" in the Backup Clients container. See "Adding Preferences" on page 267 for more information.

Creating Folders

To create a folder, click New Folder from the toolbar. Retrospect asks which type of folder you want. Your selection determines whether it is created in the My Computer container, the My Network Places container, or the Backup Clients container. After you make your choice and give it a name, the folder, identified by the ![icon] icon, appears with the volumes in the list. You can drag it to reposition it in the list.

Arranging Folders

You can drag any volume into or out of a folder to better organize the list of volumes.
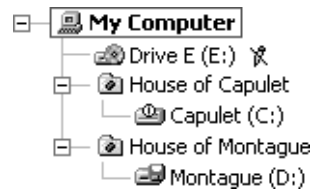
Just like folders on a hard disk, folders are useful for hiding numerous items to avoid cluttering your work space. For example, if you are administering a large number of clients, you can arrange them in a logical order by placing the individual volumes into their respective department folders, such as Accounting, Engineering, and Manufacturing. You can then select a folder in a volume selection window and Retrospect selects all the volumes within the folder.

NOTE: Each volume can only be added to *one* folder. This is different from Source Groups where the same volume can be added to more than one group.

Removing Folders

You can remove an unused folder by selecting it and clicking Forget from the toolbar or pressing the Delete key. However, you must move the contents out of the folder before you forget it.

Subvolumes

A Subvolume is a folder on a volume you define to work like a volume for use within Retrospect. After a folder is designated as a Subvolume it can be specified as a source or destination for Retrospect operations. Subvolumes have no function outside Retrospect and their mere existence does not affect a volume's files and folders in any way.

If you only want to back up files in a single folder, specifying a Subvolume (instead of specifying a volume and using a custom selector) reduces the file scanning time, minimizes the number of files displayed in a browser, and reduces the amount of memory needed.

Retrospect treats a Subvolume as another volume on your system. Once a folder has been defined as a Subvolume, do not remove or rename the folder. If you do, Retrospect will not be able to locate the Subvolume.

NOTE: Subvolumes are considered part of their parent volume when performing multiple executions. For example, you cannot back up subvolumes belonging to the same volume concurrently. If you attempt to do so, Retrospect will back up the volumes consecutively.

Specifying Subvolumes

In a volume list, select a volume, then click Make Subvolume from the toolbar or click the Subvolume button in the window. A dialog appears, listing folders at the top level of the selected volume.
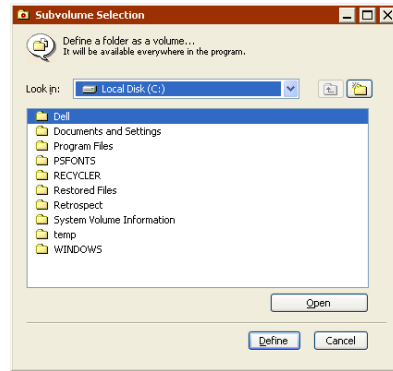
You can specify any folder on the selected volume as a Subvolume, including folders nested deep within the folder hierarchy. Select the folder you want to specify as a Subvolume and click Define. (To define the folder name currently displayed in the list box as a Subvolume, click Use.) The Subvolume folder, identified by the ▢ icon, then appears with the volumes in the volume list.

NOTE: If you specify both a Subvolume and its parent volume as Sources, they will be treated as separate objects. However, operations involving the parent volume will include the contents of the folder designated as a Subvolume.

To discard a defined Subvolume:

1. Select the Subvolume from the Volumes Database window.

2. Click Forget from the toolbar or press the Delete key.

Forgetting a Subvolume does not affect the contents of the original folder or any files you may have already backed up from it.

Volume Utilities

In the Volumes Database and volume selection windows, the toolbar has commands for defining and forgetting Subvolumes and for renaming, ejecting, erasing, and getting information about listed volumes.

TIP: Click the right mouse button in the volume list to pop up a menu of commands equivalent to the those on the toolbar.

Make Subvolume

To define a folder as Subvolume, select its parent volume and click the Make Subvolume icon or press Control+U. Use the dialog as described in "Specifying Subvolumes".

Licensing

If you purchased Retrospect SQL Server Agent or Retrospect Exchange Server Agent licenses, you must apply a license to each server you want to back up. To apply a license code to a SQL or Exchange server, select the server, then click the License icon in the toolbar, or press Alt-L.

NOTE: Local servers are listed in the My Computer container. Client servers are listed in the Backup Clients container.

Properties

To view a volume's properties, select it, and click the Properties icon or press Alt-Enter. Properties include type, file system, total and available space on the volume, and location.

Login as

The best way to ensure that all operations involving network volumes and SQL and Exchange servers will be successful is to log in to Retrospect as a user that has permissions for these resources. See "Security Preferences" on page 265 for more information.

See Appendix A: SQL Server Agent and Appendix B: Exchange Server Agent for more

information about setting up login information for SQL and Exchange servers.

You can use the Login as button if you are logged into Retrospect as a user that does not have permissions to a network volume and you want to perform an immediate operation using the volume. Select the volume in the Volumes Database list, click the Login as icon in the toolbar, and enter a user name and password.

NOTE: Automated operations using the volume may not work.

Rename

To change the name of a volume or Subvolume, select it and click the Rename icon or press Control-R. Enter a new name in the dialog that displays.

Eject

To eject removable media from a drive, select its volume name and click the Eject icon or press Control-J.

Forget

To remove a volume or Subvolume from the list, select it and click Forget from the toolbar, or click Delete. Currently active volumes, such as your hard disk or an inserted cartridge, may not be forgotten. Forgetting a server forgets its databases and defined Subvolumes.

Erase

To erase the contents of a volume, select it and click Erase or press Control-E. Be careful; this command permanently removes all files from the volume.

Browsing

The Volumes Database window has a Browse button. To view and work with the contents of a volume, select the volume and click the Browse button to open a browser. Browsing a volume is explained in detail in "Browsing" on page 286.

Windows Volume Mount Points (NTFS Mounted Drives)

Windows 2000 and Windows XP allow you designate an empty folder as a volume mount point, a kind of gateway for accessing a different drive. For an overview and configuration instructions, see the Windows 2000/XP help index under "mounted drives overview" and "mounting volumes as NTFS folders."

Appearance and Organization

In the Windows Explorer a mount point appears with a drive icon and bears the name of the folder through which the drive is accessed. Hierarchically, the mount point appears as a drive within a drive, not on the same level as other drives under My Computer.
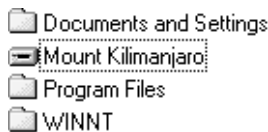
Parent volume C: in Windows Explorer

In Retrospect a mount point appears with a drive icon and bears the drive label. In Retrospect's Volumes Database and volumes selection windows, the mounted drive appears at the same hierarchy level as other drives under the My Computer container.

Mounted volumes available to Retrospect

In Retrospect's volume browser windows, browsing the parent volume of a mount point,

the mount point appears merely as the empty folder it really is.
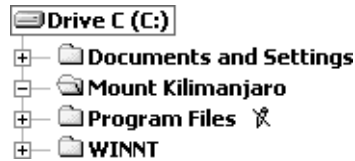
The mount point's parent volume in a Retrospect browser

Logic and Functionality

Retrospect considers a mounted drive as a distinct volume, not as a folder or Subvolume of the parent NTFS volume. To back up a volume accessed through a mount point, you must select that mounted drive in Retrospect. It will not be backed up if you select the parent drive containing the mount point folder or if you select the folder itself.

When Retrospect backs up the parent volume of a folder used as a mount point, it includes the mount point folder in the Snapshot but does not include files and folders from the mounted volume.

When Retrospect restores from a Snapshot, it restores the mount point folder and the necessary information for Windows to access its volume through the mount path. (This is dependent upon the accessed drive being present in its original state; if not, the folder is restored but it is not made a mount point.) To restore files and folders to the mounted volume, you must restore it as you would restore any other drive with Retrospect, by selecting it as a distinct drive.

BROWSING

Browsers are Retrospect's powerful tools for viewing, selecting, and manipulating files and folders on your source and destination volumes. From within Retrospect, browser windows pro-

vide file management facilities similar to those in the Windows Explorer, and include other features not available in the Explorer.

Browsers "unfold" the contents of a volume so you can work with all of its contents all at once. This lets you easily select multiple files within different folders. You can also view browsers in a flat-file structure, without the folder hierarchy.

Browsers allow you to see the files chosen for backup, restore, duplicate, and copy operations. You can also use browsers in a "stand-alone" manner to view and manage the contents of volumes. In backup, restore, duplicate, and copy operations, browsers show you which files have been chosen by the selector you designated and allow you to mark and unmark files.

You can open any number of browser windows, including different browsers for the same volume. You can also leave browser windows open while performing other Retrospect operations and switch back and forth between browser windows and other Retrospect windows.

In each browser window, Retrospect has a toolbar. It has commands for finding, selecting, and managing folders and files in the browser listing. (You can also right-click to use a contextual menu.)

Viewing a Stand-alone Browser

To view a stand-alone browser of a volume, click Configure>Volumes. The Volumes Database window appears, listing the names of available volumes. Select a volume, then click Browse. Retrospect scans the selected volume, then displays a browser window listing all the folders and files contained in the selected volume.

To view a stand-alone browser of a Backup Set, see "Viewing Session Contents" on page 233. To view a stand-alone browser of a Snapshot, see "The Snapshots tab" on page 257.

Viewing a Browser from an Operation

To view a browser within an immediate backup, restore, duplicate, or copy operation, click the summary window button named either Files Chosen or Preview. Retrospect displays a browser window for each source.

Browsers and Scripts

You cannot use a browser within a script because scripts are meant for unattended execution at a later time. Using a browser would not be useful because a volume's contents are likely to change between the time you edit the script and the time the script is executed.

About Browsers

A browser window displays a hierarchical file list of folders and files in the selected volume.
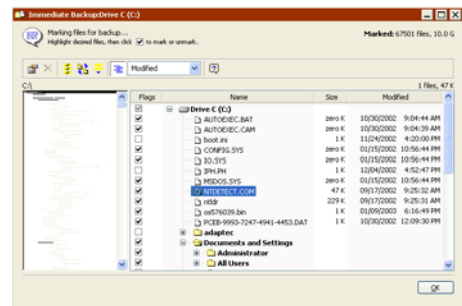
At the top of the list (and at the highest level of the hierarchy) is the name of the volume. Folders have + and − controls to their left; click + to show the contents of the folder. Click − to hide the contents of the folder. Open folders have different icons, , than closed folders, .

Folder contents hidden (left) and exposed (right).

The scrolling folder index on the left of the window provides a thumbnail view of the folders on the volume. Click on the folder index to display the associated file list on the right side of the

window. The pathname of the current selection is shown above the index. Index lines appear grey for unopened folders or black for open folders.

The upper right corner of the window indicates how many files are highlighted or marked and shows their total size.

Selecting Files and Folders

In a browser window, you select files and folders on which to perform operations. Select files by clicking on entries in the file list. Drag through the list or Shift-click to select a range of files or folders. Control-click to select or deselect non-contiguous items. Select all items by choosing Select All from the Edit menu. Double-clicking a file both selects (highlights) and marks it. Marking is described below, under "Marking Files and Folders."

Getting Additional Information

Retrospect provides a Properties command you can use to view information about the selected files and folders.

To View Information About Files or Folders:

1. From a browser, select the files or folders for which you want more information.

2. Click Properties from the toolbar.

A properties window appears for each selected file or folder, displaying additional information.
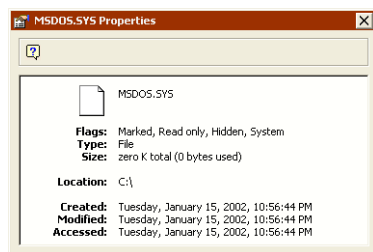
Marking Files and Folders

A marked file or folder is one that is designated to be used in some way (for example, backed up, archived, duplicated, or restored). When performing operations, Retrospect marks files according to the rules of the selectors in the search criteria, but you have no way of knowing which files are marked unless you use browsers. In addition to simply viewing a list, you can manually mark and unmark files and folders within a browser.

Marked files indicate the files you want Retrospect to evaluate when performing an operation. Not all the marked files will be backed up (or duplicated, restored etc.). For example, during a backup using Retrospect's default settings, only new and modified files will be backed up, regardless of which files you mark. Retrospect displays a diamond icon in the browser list next to source files that already exist on the destination. These files will not be copied to the destination again, saving time and media space.

You mark files and folders in a browser by selecting them and clicking the checkbox to the left of a file or folder. Click a checked checkbox to unmark the item. You can also mark and unmark files and folders by double-clicking them.

To mark or unmark an item without affecting the highlighting of other items, press and hold the Control key while clicking.

By marking or unmarking a folder you perform the same operations on all the files (and folders) contained within that folder. For example, to specify a single folder for backup, you would double-click on the volume name at the top of the file list to unmark all of the files, then scroll to the folder you want to back up and double-click the folder icon to mark it and its contents.

The browser window's toolbar provides additional commands for highlighting and marking in the window.

Highlight Marks: highlights marked files. If you click or double-click an item without hold-

ing the Control key you may end up unhighlighting marked items. This command is useful for rehighlighting them.

Cross Reference: allows you to locate files in the same hard disk or session that are related to a specified file. Specifically, Cross Reference finds duplicate files, older versions of the same file, and even files that have been renamed but were originally from the same file. This command highlights, but does not mark, cross-referenced files.

Selecting View Formats

Click the Hierarchical/Sorted View button on a browser window's toolbar command to change how Retrospect displays the contents of a volume.

The hierarchical format displays files and folders in the same hierarchical structure in which they are stored on the volume. This is the default layout that Retrospect uses when you first open a browser window.

The sorted files format displays all files stored in the selected volume as a single "flat file" list, discarding any folder designations.

For both types of browser layouts, the toolbar's list box allows you to specify the type of file information displayed in the browser window. It always displays flags, name, and size. For the final piece of information you can choose modification date/time or attributes.

With the sorted files layout, you can choose the sort criterion of the list by clicking on a column heading. Clicking it a second time reverses the sort order. Retrospect normally sorts the files in ascending order. For example, if sorting by size is specified, the browser lists the smallest files at the top of the list and largest files at the bottom.

Finding Files

The Edit menu has a Find item that you can use to locate specific files or folders (but not empty folders) on the volume.

NOTE: Restoring by searching uses the same window as the one described below.
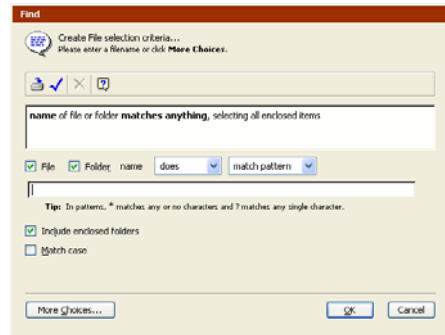
The Find window (showing fewer choices).

This basic find window considers a file or folder name as the primary search criterion. Click More Choices to build a custom selector to use other criteria. The window that appears is identical to the selector details window you use to build Retrospect selectors.

For more information on using the Find window to build search conditions, see "Using Selectors" on page 291.

In the text entry field, type the text to use in your criteria. It is not case-sensitive unless you click the Match case check box.

Use the File and Folder checkboxes to consider or disregard files and folders while searching. When you consider folders, check "Include enclosed folders" to select all enclosed items of found folders, including files nested in other folders.

Use the "does/does not" list box to control the search logic. "Does" is inclusive; "does not" is exclusive. For example, if you choose "does not," and perform a search on file names,

Retrospect selects all the files and folders whose names do not contain the search text.

Use the other list box to specify where the search text is positioned within the name. You can specify that the search text be located at the beginning (start with) or end (end with) of the name, or contained somewhere within a name (contain). You can specify that the name exactly match the search text and no additional text (match). Or you can specify that the name matches a pattern (match pattern) of the search text. When matching a pattern, you can use the wildcard character ? to match any single character, and use the wildcard character * to match multiple characters.

After you edit the search criteria in the find window and click OK, Retrospect highlights all files and folders that meet the search criteria. You can then mark the highlighted files for use in your operation.

Printing or Exporting a File List

Any time a browser window is active, you can print the contents of the file list or export it to a file. To print, choose Print from the File menu. If you use Page Setup to reduce the printing size, Retrospect will print a browser in more than one column to save pages. To export to a text file, choose Export from the File menu. Retrospect exports the fields in the following order, regardless of the view format: file name, size, create date, create time, modify date, modify time, backup date, backup time, Mac OS type, Mac OS creator, Backup Set (if any), and path.

Copying and Pasting Selections

You can copy selections between browser windows. When you copy a selection, only the file and pathname information is copied, not the files themselves. This feature is useful for copying selections from a stand-alone browser window into a browser window opened during a Retrospect operation such as restore.

NOTE: You cannot paste a copied selection into any other applications or documents.

To Copy Selections Between Browser Windows:

1. Make your file and folder selection then choose Copy from the Edit menu.

2. Open (or bring to the front) the appropriate browser window for the same volume.

3. Choose Paste from the Edit menu.

Retrospect pastes the selection into the new browser window, highlighting only the same files and folders (in the same folder hierarchy) that were selected and copied in the other browser window.

Saving Selections as a Selector

You can also save file and folder selections as a selector that you can use to reselect files for future Retrospect operations on the same volume, including backups and restores.

NOTE: Before you save a selection as a selector, consider creating a custom selector as described in "Using Selectors" on page 291. You can easily review and modify custom selectors at any time. A selector created with a browser's Save Highlights command is less flexible.

To Save Selections as a Selector:

1. Select the files/folders you want to apply to a selector.

2. Click Save Highlights from the toolbar.
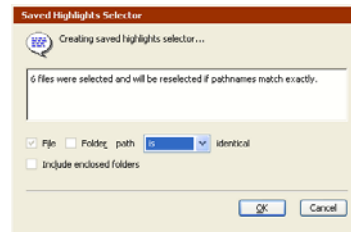
The window that appears tells you how many files were selected and will be selected by this selector if pathnames match exactly.

3. Use the list box to control whether the saved selector is inclusive or exclusive.

This window also includes file and folder options similar to those in the find window, as described in "Finding Files" on page 289.

4. Click OK then enter a selector name to save your new selector.

Rescanning a Volume

You can update the contents of the browser window by choosing Refresh from the File menu. This is useful, for example, if you make changes to the volume (for example, in the Windows Explorer or another browser window) while the volume's browser window is open.

The Refresh item appears in the File menu only when Retrospect is working with a volume directly. For example, you can not rescan a volume when you are browsing a Backup Set.

Deleting Files

Retrospect browsers have a Delete command to remove files from a volume, which is like placing a file in the Windows desktop's Recycle Bin and emptying it.

NOTE: Retrospect does not allow you to delete files from a Backup Set.

To Delete Files:

1. Select the file or files you want to delete in the file list.

2. Click Delete from the toolbar.

A dialog appears, asking you to specify whether you want to remove the selected files only or remove the selected files and any empty folders that may result from the file deletions.

3. Make your choice, then click OK.

Retrospect permanently deletes the selected files from the volume.

WARNING: A delete command may not be undone with the Undo command, nor may a file

be pulled from the Recycle Bin. When a file is deleted, it is gone.

The browser window toolbar has Delete enabled only when Retrospect is working with a volume directly. For example, you can not delete a file when you are browsing a Backup Set.

USING SELECTORS

You can use selectors with immediate and automated operations to specify the types of files and folders you want the operation to include. Using selectors to intelligently select certain files and folders you can limit the amount of time and media required for an operation.

Selectors let you choose files based on almost any criteria, including name, date, type, or size. Retrospect includes a number of built-in selectors, and you can also create custom selectors. For example, you can create a selector that will choose all text documents modified after October 15, 2004.

A file that is marked by a selector will not necessarily be copied to the destination. All copying operations (such as backups) using selectors are "smart," or progressive, because of Retrospect's matching feature. For each selector, there is the implied meaning of "select this file, but do not copy it if it already exists in the destination."

NOTE: Retrospect's selectors do not select empty folders.

The Selectors Window

You create and modify selectors through Retrospect's selectors window.

To display the selectors window, click Configure>Selectors. The selectors window lists all of the built-in and custom selectors.
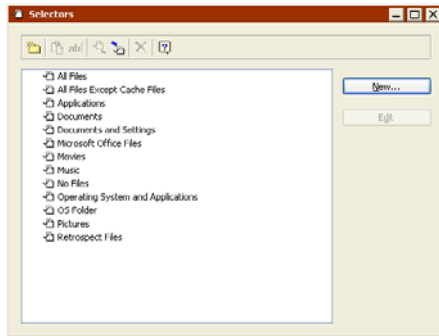
The selectors window has two buttons for working with the selectors.

New creates a new selector.

Edit allows you to add new conditions or modify existing conditions for a selector.

The selectors window includes a toolbar with the following commands:

New Folder makes a folder container for organizing selectors.

Duplicate makes a copy of the currently highlighted selector.

Rename lets you change the name of the currently highlighted selector.

Export lets you export selectors to a file. For example, you can create a custom selector for use with Retrospect on one backup computer, then export the selector for use with another copy of Retrospect running on a second backup computer.

Import lets you import selectors from a file.

Delete removes the currently highlighted selector.

TIP: Click the right mouse button in the selectors list to pop up a menu of commands equivalent to the those on the toolbar and the buttons in the window.

Built-in Selectors

Retrospect includes a number of built-in selectors, with predefined conditions for selecting files.

NOTE: Some selectors and selector conditions function differently with Windows, Mac OS, NetWare, and UNIX volumes. The descriptions below focus on how the built-in selectors interact with Windows volumes. To determine how the selectors work with other operating systems, double-click on a selector to view its details, or check the selector on a non-Windows volume. See "Selector Toolbar" on page 299 for more information on checking selectors.

Retrospect's built-in selectors are:

All Files marks all files on the source, including the operating system folder. This is the default selector.

All Files Except Cache Files marks all files on the source, except cache files used by certain applications, such as web browsers. These cache files, which are often large, are not needed for restoring.

Applications marks only executable applications (.exe) and code libraries (.dll), except those that reside in the system folder.

Documents marks files that are not executable applications (.exe) or code libraries (.dll), and which do not reside in the Program Files folder or in the operating system folder, except for files within the Desktop and Favorites folders.

Documents and Settings marks files in the Documents and Settings folder, which contains every user's folders including My Documents, Favorites, Application Data, and Desktop.

NOTE: For Windows 9x systems, the "Documents and Settings" selector marks the Profiles folder.

For Mac OS X, this selector marks the Users and Library/Preferences folders.

Movies marks files with common movie file extensions (.mov, for example) anywhere on the source, except the Windows and Program Files folders. It also marks all files in the My Documents\My Videos and Movies folders for all users.

Music marks all files in the My Documents\My Music folder for all users. It also marks files with common music file extensions (.mp3, for example) anywhere on the source, except the Windows and Program Files folders. This selector also marks the Music folder for all users on Mac OS X and Windows computers (if the folder exists).

No Files does not mark any files.

Office Documents marks Microsoft Office Documents, Microsoft Outlook data, and Adobe PDF files anywhere on the source, except the Windows and Program Files folders.

Operating System and Applications marks system files, including the Windows folder and the System State. Also marks application files, including everything in the Program Files folder, as well as files with known application extensions (like .exe and .dll) anywhere on the source.

OS Folder marks files within the operating system folder. For UNIX, this selector marks no files.

Pictures marks all files in the My Documents\My Pictures folder for all users. It also marks files with common picture file extensions (.jpg, for example) anywhere on the source, except the Windows and Program Files folders. This selector also marks the Pictures folder for all users on Mac OS X and Windows computers (if the folder exists).

Retrospect Files marks catalogs, logs, configurations, and other documents related to Retrospect. For UNIX, this selector marks no files.

All Files is the default selector used for immediate operations and scripts. You should use this selector to ensure complete backups.

To view details about a selector, click on it to select it in the Selectors window and click Edit (or just double-click the selector), which brings up a window with the selector's conditions.
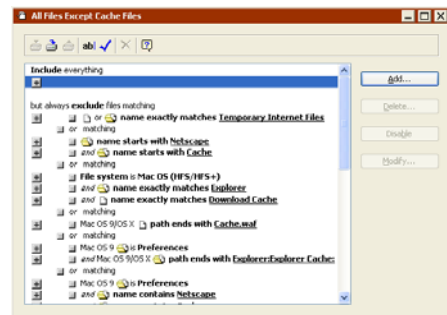
See "Selector Conditions" for help understanding the conditions that make up a selector.

Selector Conditions

A selector is made up of a combinations of conditions that include or exclude files and folders that meet certain criteria. Retrospect includes many detailed conditions that allow you to create sophisticated selectors.

To view or modify selector conditions, select a selector from the Selectors window, then click Edit. The selector details window appears. It includes one section for adding conditions to include certain files and folders and another section for adding conditions to exclude certain file files and folders.
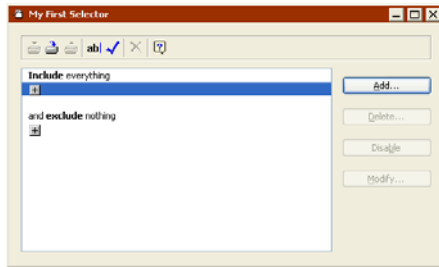
Click the + button underneath the Include or Exclude heading to display the Condition window.
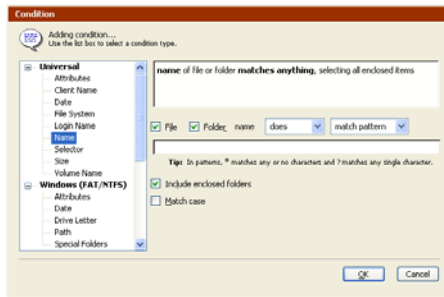
Along the left of the Condition window, Retrospect lists the categories of conditions available:

- Universal Selector Conditions
- Windows Selector Conditions
- Mac OS Selector Conditions
- UNIX Selector Conditions
- NetWare OS Selector Conditions
- Mailbox Selector Conditions

Universal Selector Conditions
Universal conditions work with all supported file systems. You can build your own selectors using the following conditions.

Attributes (Universal) uses read-only and hidden attributes, in addition to Retrospect's marked and matched attributes.

Client Name (Universal) uses the name from Retrospect's client database as the condition.

Date (Universal) uses creation, modification, or backup dates as conditions.

File System (Universal) uses the source volume's file system as the condition.

Login Name (Universal) uses file sharing owner, group or login names as the condition.

Name (Universal) uses the name of the file or folder as the condition.

Selector (Universal) uses another selector as the condition.

Size (Universal) lets you specify file or folder size as the condition.

Volume Name (Universal) uses the name of the volume as the condition. For Windows volumes, this is the volume label shown in its properties, not the drive letter.

Windows Selector Conditions
Windows conditions work with FAT and NTFS file systems. You can build your own selectors using the following conditions.

Attributes (Windows) uses archive, system, encrypted, and offline flags as conditions.

Date (Windows) uses Windows-specific date attributes as conditions.

Drive Letter (Windows) uses the source volume drive letter as the condition.

Path (Windows) uses the path to the file or folder as the condition. Folder hierarchy is delineated by the "\" character.

Special Folders (Windows) uses certain system-defined folders, such as Volume Root and Documents and Settings, as conditions.

Mac OS Selector Conditions
Mac OS conditions work with HFS and HFS+ file systems. You can build your own selectors using the following conditions.

Attributes (Mac OS) uses file attributes (file busy, alias, name locked, stationery, or custom icon) as the conditions.

File Kind (Mac OS) uses file creator and type as conditions.

Label, Icon Color (Mac OS) uses a file or folder's label as a condition. The Label menu or submenu in the Finder contains seven labels (and colors, if your monitor displays colors or shades of gray) and the "None" option. Each checkbox in this window corresponds to a specific item position in the Label menu and not to the actual color or label name.

Path (Mac OS) uses the path to the file or folder as the condition. Use a colon (:) as the separator in path names for both Mac OS X and Mac OS 9 and earlier. Path names must include the volume.

Permissions (Mac OS): Read, write, and execute permissions for user, group, and other. Mac OS X file/folder permission much match the condition exactly (with * used as a wildcard). For example, to select all files that can be written to by either user, group, or other, you would need to create three separate "or" conditions: *w*******, ****w****, and *******w*.

Special Folders (Mac OS) uses certain system-defined folders, such as the Volume Root and Control Panels folder, as conditions. These conditions are only for use with Mac OS 9 and earlier.

UNIX Selector Conditions

UNIX OS conditions work with UNIX file systems. You can build your own selectors using the following conditions.

Attributes (Unix OS) uses file attributes (symbolic link flag settings) as the conditions.

Date (Unix OS): UNIX-specific date attributes

Path (Unix OS): Path to the file or folder. Folder hierarchy is delineated by the "/" character.

Permissions (Unix OS): Read, write, and execute permissions for user, group, and other. UNIX file/folder permission much match the condition exactly (with * used as a wildcard). For example, to select all files that can be written to by either user, group, or other, you would need to create three separate "or" conditions: *w*******, ****w****, and *******w*.

NetWare OS Selector Conditions

NetWare OS conditions work with NetWare files systems. You can build your own selectors using the following conditions.

Date (NetWare OS) allows you to create a selector to include or exclude files/folders from a backup based on access date and time or status modified date and time.

Path (NetWare OS) allows you to create a selector to include or exclude files/folders from a backup based on their location on the NetWare server.

TIP: To *exclude* folders from a backup, you should use the `retroclt -exclude` option described in "NetWare Client Command Line" on page 187.

Mailbox Selector Conditions

Mailbox conditions can be used when backing up or restoring Exchange mailboxes.

Sender uses the sender of the message as the condition.

Working with Conditions

Each condition type has its own controls for entering and specifying details for the condition.
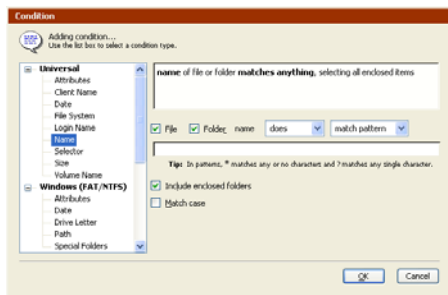
When you add or change a condition it appears in the selector detail window.
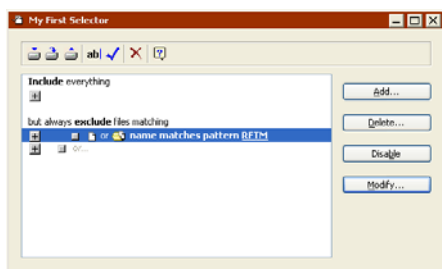
You can add multiple conditions to a selector by clicking the + conditions buttons. The location of the + button determines the relationship between the conditions; it may add a condition with the And operator or may add a condition with the Or operator. When you click a + button to open a condition window, the window shows its operator type so you know whether you are And-ing or Or-ing a new condition.

The And operator allows you to combine conditions so that a file or folder must meet the combined conditions before it is selected. Each condition uses an And operator, except each final condition of the Include and Exclude areas.
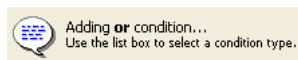
The Or operator allows you to build conditions where a file or folder must meet at least one

condition—but not necessarily all conditions—before it is selected. The last condition under each Include and Exclude area always uses an Or operator.

Click on this button to add an "And"
condition to the "name" condition.
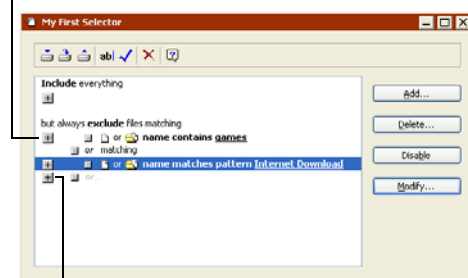
Click on this button to add an "Or"
condition to the Exclude area.

To gain a better understanding of how this works, see "Creating a Custom Selector" on page 297 and experiment with conditions on your own.

Condition Examples

The table below shows an example of a custom selector and its effect when applied to some files.

Condition Rules

Exclude statements always take precedence over Include statements when Retrospect applies the selector. For example, if a selector has a statement which includes the Profiles folder and a statement which excludes the OS Folder, the files in the Profiles folder will not be marked.

Creating a Custom Selector

Retrospect allows you to quickly build selectors that can perform sophisticated file and folder selection. The best way to learn about custom selectors is to create one. In the following example, you create a custom selector that excludes certain applications and a folder called "Games" from backup.

Creating a New Selector

From the navigation bar, click Configure> Selectors button, then click New. Retrospect prompts you to name the new selector. This example uses "Unwanted games and apps" but you can enter a name of your own.
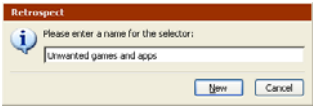
After typing the name, click New. Retrospect displays a selector details window for the new selector. Notice the window name is the selector name.
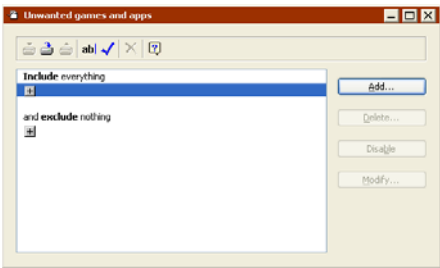
By default, new selectors include everything and exclude nothing, until you add conditions.

Excluding Files

Click the + button beneath the exclude heading to add a condition. In the condition window that appears, select the Windows Special Folders condition to specify a folder type to exclude.
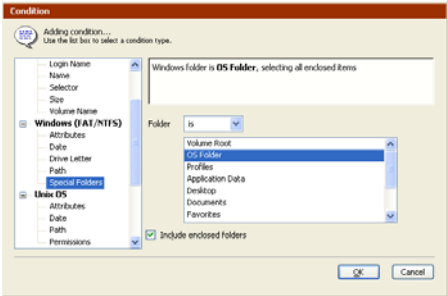
Using this Selector	On these Files	Marks these Files
Include files matching ⊞ ☐ 🗋 **name contains _something_** ☐ _or_ matching ⊞ ☐ 🗋 **name contains _nothing_** ⊞ ☐ _or..._	nothing can survive in a vacuum some things I'd like to say something for nothing something more to give	nothing can survive in a vacuum something for nothing something more to give
Include files matching ⊞ ☐ 🗋 **name contains _nothing_** ⊞ ☐ _and_ 🗋 **name contains _something_** ⊞ ☐ _or..._	nothing noble in your fate something breaks the silence something for nothing	something for nothing

Select Application Data and click OK. The selector details window now reflects our new condition.
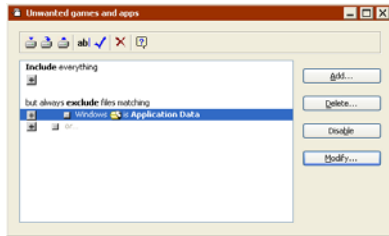
At this point, the selector excludes the application data folder on Windows volumes. You are now ready to add a second condition.

Click the second + button below the exclude heading, which has the word "or" next to its ☐ handle icon. In the condition window that appears, select the Mac OS File Kind condition.

Condition description   **File type entry box**
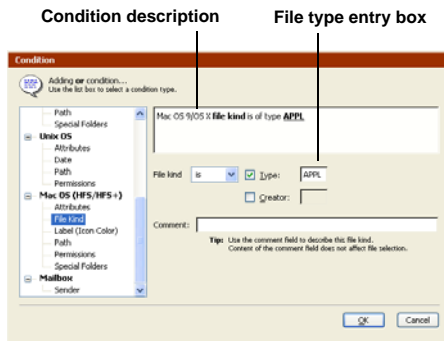
This window lets you specify a file type and/or creator as a condition. The default file kind is a generic application with the type "APPL." Since this is the condition we would like to use in this example, click OK. The selector details window now reflects our new condition.
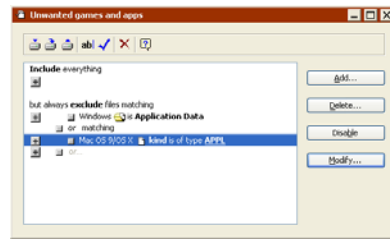
Because we added this condition from the lowest + button, Retrospect added the condition to the selector with the Or operator. Or and And operators are explained in "Working with Conditions" on page 295.

We are ready to add a third condition. Click the lowest + button beneath the exclude heading, then select the Universal Name condition in the condition window.

Condition description   **Text box for entering name**
                              Logical decision
                              Text matching action
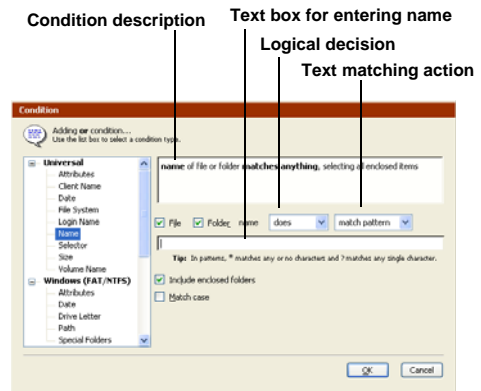
Choose contain for the text matching action and enter "games" in the text box. Leave the other controls as they are. Click OK to return to the selector details window.
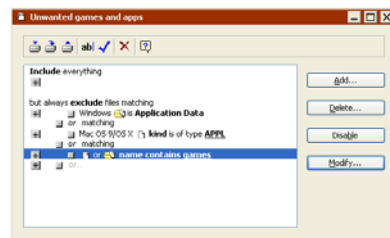
At this point, the selector excludes the contents of the Windows application data folder, all Mac OS applications, and any folder containing the word "games."

You can save this selector and use it in scripts, immediate operations, and browsers.

Selector Toolbar

The selector details window includes a toolbar with the following commands.

Save: This saves the selector using its current name, replacing what was last saved.

Save As: This lets you save the selector using a different name. Enter the new name in the dialog which follows, then click Save. The original selector remains as it was when it was last saved.

Revert: This lets you discard your current changes to a selector and revert it back to its last saved state.

Rename: This lets you change the name of the selector. Enter the new name in the dialog, then click Rename.

Check Selector: This lets you test your selector by applying it to a volume. Retrospect asks you to select a volume for browsing with your selector. Do so and it opens a browser window with the files that match the selector criteria marked with checks. The marked files are the ones Retrospect would back up when using this selector.

If the correct files are marked, the selector is working properly and you can begin using it for immediate operations or in scripts.

If the files that are marked are not the correct ones, you need to modify your selector and check it again. You may need to add conditions, delete conditions, or modify the conditions. Pay close attention to the And and Or operators which affect the results of your selector. When

you have finished modifying your selector, save it and check it again to see if the correct files are now marked. Repeat this process as needed until your selector is working correctly.

Delete: This lets you delete the selected condition from the selector.

Printing a Selector

You can print the contents of selector details windows to keep for reference. To print a selector window, edit the selector and choose Print from the File menu.

Modifying a Selector

Any condition that appears in a selector details window can be modified. After you modify a condition, Retrospect returns to the selector details window, where you can add new conditions or modify existing conditions.

To open a selector from the selectors window, click on the selector you want to modify then click Edit (or just double-click the selector). Retrospect opens the details window for the selector.

To edit a selector's existing condition, select it and click Modify, or just double-click the condition line (except on the + and ▣ icons). In the condition window, you can modify its options and controls. Click OK to accept the changes to the condition.

To add a new condition, click a + icon. (Remember, the + next to the ▣ handle with the grayed-out "or..." adds an "Or" condition, while the other + icons add an "And" condition.) A condition window appears, providing options and controls for the type of condition you chose. Make the appropriate choices and settings in the window then click OK to add it to the selector. The condition window closes and the selector window now displays the new condition.

Disabling Conditions

At any time, you can disable a condition within a selector. When a condition is disabled, it has no effect on file selection and will remain inactive until it is enabled. This feature is useful when a selector becomes very complex and you want to resolve problems by testing parts of it.

To disable a condition, first open a selector and select the condition you want to disable. Click Disable and Retrospect disables the selected condition, displaying it in grayed out text to identify it as inactive.

You can restore a disabled condition by selecting the condition and clicking Enable.

Moving Conditions

Within a selector details window, you can move a condition by dragging the ▣ handle next to the condition description and dropping it at a new location within the window's scroll box.

You can drag any condition to a new location, either in the same group or another group or heading. For example, if you added a name condition under the Include heading, you can change the same condition to an exclusionary condition by dragging it beneath the Exclude heading.

When you move a condition, its outline follows the hand cursor, indicating the new location for the condition. Release the mouse button when a new outline appears in your desired destination. After you drop it, Retrospect moves the condition to the new location, inserting it before the outlined destination condition.

To copy the condition, press and hold the Shift key while dragging. Dragging an "or matching" heading moves the entire group. Shift-dragging an "or matching" heading copies the group.

NOTE: Be careful to pay attention to the operator type (And or Or) of what you are dragging; moving it may change the operator.

Removing Conditions

At any time, you can remove a condition from within a selector.

To delete a condition, first open a selector and select the condition you want to remove. Click Delete and confirm to remove the selected condition from the window.

Deleting a Selector

If you no longer need a selector you can delete it through the selectors window.

To delete a selector, click on the selector to select it, then click Delete from the toolbar or press the Delete key. A dialog appears asking you to confirm the deletion. Click OK. Retrospect deletes the selector.

Duplicating a Selector

Sometimes, you will want to duplicate a selector so that you can make slight modifications to fit your needs. For example, you may want to modify a copy of one of Retrospect's built-in selectors but leave the original untouched. You can make a duplicate through the selectors window.

To duplicate a selector, click on the selector to select it, then click Duplicate from the toolbar. A dialog appears providing a field for entering a new selector name. Type a new name and click New. Retrospect creates an exact copy of the selector, using the name you provided in the dialog.

Selector Examples

Following are some examples of selectors and detailed explanations of each.

Network Backup Selector

This selector marks all documents to be backed up, except for files in a folder named "Games" on Leslie's client computer. In this example, the backup administrator knows that Leslie has a

large folder with games that do not need to be backed up.
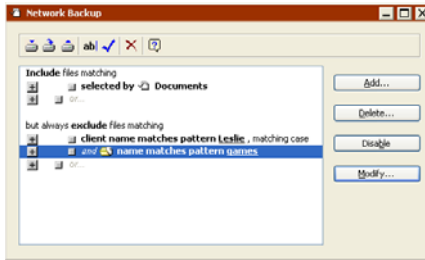
Restore Searching Selector

This selector uses a date condition to search for an Acrobat PDF document file that was modified on or after October 17, 2001 at 5:04 P.M. It uses a name condition to find it on a Windows volume and uses a file kind condition to find it on a Macintosh volume. This selector is a good example of how, during an immediate restore operation, you could have Retrospect find a file when you forgot its name. Even though you do not know the exact file name, you know the file was last saved after a certain date and time.
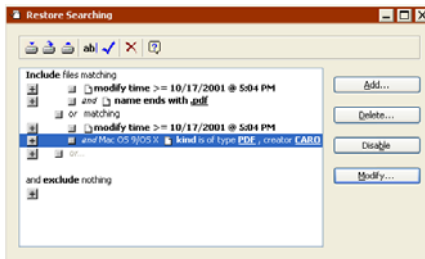
Client Restore Searching Selector

This selector searches for a named file that was created on a particular client user's computer. In this case, the name of the file is "Dissertation" and client's name is "Neil." This selector could be used during an immediate restore operation.
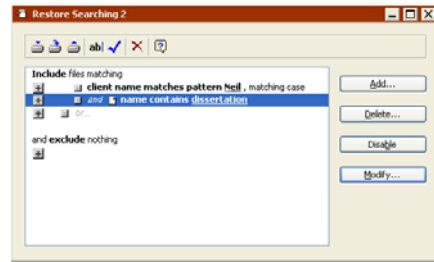
MAINTENANCE AND REPAIR

This section provides instructions for maintaining and repairing catalogs and media by performing the following tasks:

- Updating catalogs that are out-of-date or "out of sync".
- Recreating catalogs that are missing or damaged. (If it produces "chunk checksum" errors, it is damaged.)
- Repairing damaged file Backup Sets.
- Verifying Backup Set media integrity to confirm that all files are readable.

To perform these tasks, first click Tools from the navigation bar.

Updating a Catalog

You should update a Backup Set's Catalog when Retrospect reports a "catalog out of sync" error while operating with the Backup Set. You must update the Catalog to synchronize it with the media or you will be unable to use the Backup Set.

A "catalog out of sync" error indicates Retrospect was unable to update the Catalog the last time it copied data to this Backup Set—possibly because of a crash or power failure. This error may also be caused by a full disk or by a lack of memory.

NOTE: If, after updating a Catalog, you continue to get "out of sync" errors when using the Backup Set, do not attempt to repair the

Catalog again. You must skip to new media, reset with a full or new backup, or create a new Backup Set. See page 333 for more information on the error message.

To Update a Catalog:

1. Click Tools>Repair Catalog from the navigation bar.
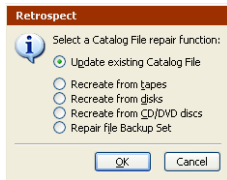
2. Select Update existing Catalog File then click OK.
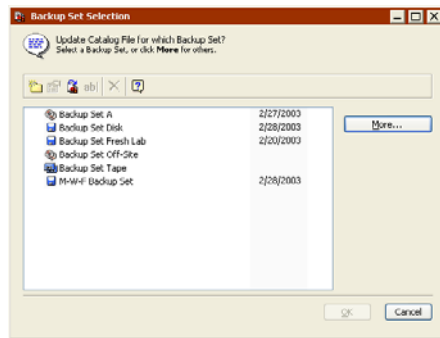
3. Select the Backup Set to update and click OK.

4. If Retrospect cannot find the most recent member, it displays a media request window.

Insert the requested media.

5. Retrospect displays a dialog asking if there are any other members in the Backup Set.
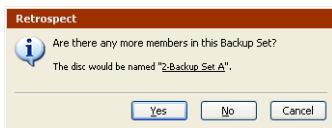
If there are no more members, click No to begin recataloging.

If there are more members in the Backup Set, click Yes. Retrospect continues to ask you for additional Backup Set members until you click No or Done.

6. Retrospect recatalogs the Backup Set, informing you of its progress in the Activity Monitor.

7. Click the History tab in the Activity Monitor for details on whether the update was successful.

If the operation was not successful, click the Log button for additional information.

Recreating a Catalog

You cannot use a Backup Set unless it has a Catalog File, so you should recreate the Catalog whenever the original Catalog File is lost or damaged. Retrospect can recreate a Catalog by reading the Backup Set media. Recreating may take a long time, depending on the amount of data in the Backup Set.

The procedure for recreating a Catalog for a disk Backup Set is different from the procedure for tape and CD/DVD Backup Sets.

Recreating a CD/DVD or Tape Catalog

Before you begin make sure to load the most recent Backup Set member for the Catalog you are recreating into the backup device.

To recreate a CD/DVD or Tape Catalog:

1. Click Tools>Repair Catalog from the navigation bar.

2. Select Recreate from tapes or Recreate from CD/DVD discs and click OK.

The Media Selection window displays.
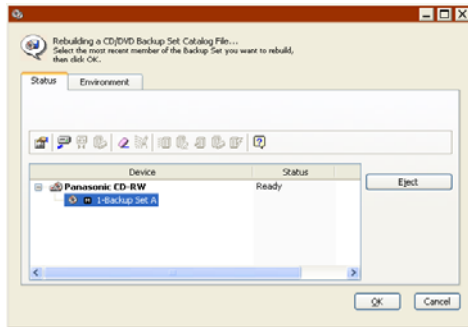
3. In the Media Selection window, click the Status tab, then select the most recent member of the Backup Set.

NOTE: For a Backup Set created with Retrospect 5.0 or 5.1, it requests the first member of the set.

If you do not have the most recent medium, insert the most recent available member of the Backup Set to be recataloged.

4. Click OK.

If you are recreating a Catalog for a Backup Set that is still known by Retrospect, it asks whether you want it to recognize the recreated Backup Set instead of the known Backup Set. Click OK to replace the known Backup Set.

5. If the Backup Set is encrypted, Retrospect asks for its password. Enter the password and click OK.

6. Specify a location to save the recreated Catalog File and click Save.

Retrospect recatalogs the Backup Set, informing you of its progress in the Activity Monitor. When Retrospect finishes recataloging a particular member of a Backup Set it asks if there are any more members to recatalog.
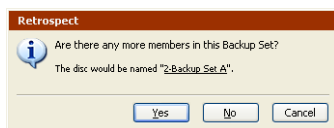
7. If there are no more members because you have already given Retrospect the final medium in the Backup Set, click No to complete the recataloging.

If there are more members in the Backup Set, *even if one or more members are lost or damaged,* click Yes.

8. Insert the requested member of the Backup Set, or if you do not have it, click Choices.

A dialog asks what happened to the member.
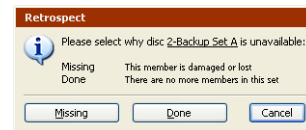
If you have already given Retrospect the final medium in the Backup Set, click Done. If you do not have the requested Backup Set member, or if it is damaged, click Missing.

9. Retrospect continues to ask you for additional Backup Set members until you click No or Done.

Click the History tab in the Activity Monitor for details on whether the recatalog was successful. If the operation was not successful, click the Log button for additional information.

NOTE: After Retrospect informs you the recataloging was successful, you should edit the scripts that used the Backup Set and add the newly-recognized, recreated Backup Set to each script.

Recreating a Disk Catalog

If you are recreating a Catalog from removable disks, make sure to load the most recent Backup Set member for the Catalog you are recreating into the backup device before you begin.

To recreate a Disk Catalog:

1. Click Tools>Repair Catalog from the navigation bar.

2. Select Recreate from disks and click OK.
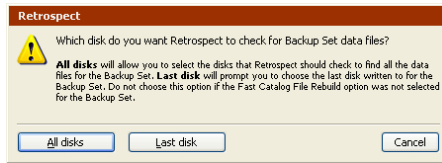
3. If you know which disk was most recently used to store the Backup Set data, click Last disk. If you are not sure, click All disks.

WARNING: Do not select Last disk if this Backup Set's Fast Catalog File rebuild option was turned off.
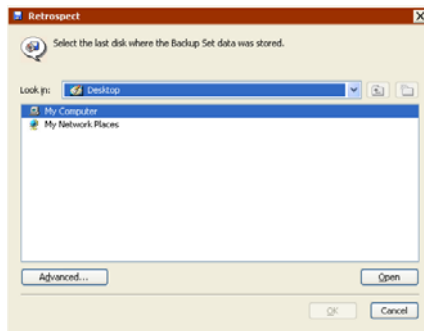
4. Browse to the location of the disk, select it, and click OK.

Retrospect displays a list of the Backup Sets on the disk.
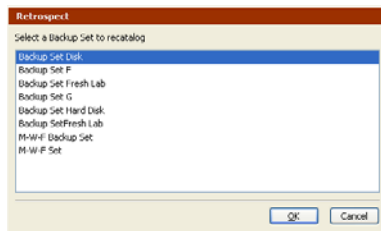
5. Select the Backup Set to recatalog and click OK.

If you selected All disks, Retrospect asks if there are any more disks in the Backup Set. If there are, click Yes and select another disk. Retrospect continues to ask you for additional disks until you click No.

6. If you are recreating a Catalog File for a Backup Set that is still known by Retrospect, it asks whether you want it to recognize the recreated Backup Set instead of the known Backup Set. Click OK to forget the known Backup Set.

7. If the Backup Set is encrypted, Retrospect asks for its password. Enter the password and click OK.

8. Specify a location to save the recreated Catalog File and click Save.

Retrospect recatalogs the Backup Set, informing you of its progress in the Activity Monitor window. When Retrospect finishes, click the History tab in the Activity Monitor for details on whether the recatalog was successful. If the operation was not successful, click the Log button for additional information.

NOTE: After Retrospect informs you the recataloging was successful, you should edit the scripts that used the old Backup Set and add the newly-recognized, recreated Backup Set to each script.

Repairing a File Backup Set

The Catalog File for a file Backup Set is stored in the same file as the Backup Set data. In order to repair a file Backup Set Catalog, you must have access to the Backup Set.

To repair a file Backup Set:

1. Click Tools>Repair Catalog from the navigation bar.
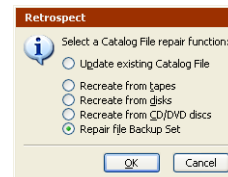
2. Select Repair file Backup Set and click OK.

Retrospect displays the Backup Set selection window.

3. Locate the file Backup Set that needs repair, select it, and click Open.

A message asks you to confirm the repair.

4. Click Yes to repair the Backup Set.

5. If the Backup Set is encrypted, Retrospect asks for its password. Enter the password and click OK.

Retrospect recatalogs the Backup Set, informing you of its progress in the Activity Monitor window. When Retrospect finishes, click the History tab in the Activity Monitor for details on whether the recatalog was successful. If the operation was not successful, click the Log button for additional information.

Incomplete Catalog Repair

When you stop a cataloging operation, the following dialog may appear.

Revert stops recataloging and allows you to continue updating the Catalog from the current medium later. (To continue later, use the Update existing Catalog File function.)

Save should be used when you do not wish to try to catalog any more data from the current medium. All data cataloged so far should be retrievable. (To continue later, use the Update existing Catalog File function.) Recataloging will resume with the next medium, if there is one. If you back up more data to the Backup Set after using this option, Retrospect will ask for a new medium, treating this one as full.

Verifying Backup Set Media

If you want to manually verify your Backup Set media, choose Tools>Verify Media from Retrospect's navigation bar. Verify Media is useful for performing offline verification of your Backup Set media after an immediate backup (or archive) that did not use verification.

TIP: You should use verification scripts to schedule offline verification if you want to maximize your backup window by running scripted backups (or archives) without verification. See "Scripted Verification" on page 132 for more information.

Whenever possible, Verify Media verifies data on Backup Set media by comparing the files in the selected Backup Set to MD5 digests generated during the backup. This means that Retrospect does not need to access the backed up source volumes, which prevents slowdowns on those volumes.

In certain circumstances, Retrospect does not have access to MD5 digests generated during backup. This is true for all backups created using versions of Retrospect prior to Retrospect 7.5, as well as backups that took place when Retrospect's "Generate MD5 digests during backup operations" preference was disabled. See "Verification Preferences" on page 270 for more information.

In these cases, Retrospect still checks all files on the Backup Set media to make sure that they are readable.

NOTE: Verify Media *does* require you to reinsert media when verifying backups that span media.

To verify media integrity:

1. Click Tools>Verify Media.

Retrospect displays the Backup Set selection window.

2. Select the Backup Set to verify, and click OK.

Retrospect verifies the Backup Set media, informing you of its progress in the Activity Monitor window.

If the Backup Set uses CD/DVDs, removables disks, or tapes, Retrospect asks you to insert each Backup Set member as it is needed.

If you do not have the requested Backup Set member, but have other members of the Backup Set to verify, click Choices, then OK, and insert the next requested piece of media.

3. When Retrospect finishes, click the History tab in the Activity Monitor for details on whether the recatalog was successful. If the operation was not successful, click the Log button for additional information.

NOTE: Consider backing up unverified files to a new Backup Set.

4. Click Done.

EXTERNAL SCRIPTING

Retrospect events can be handled by external scripts, which you can author in any scripting language that can create executable files. You can attach a single executable script to Retrospect or to a Retrospect client to act upon the events.

This section assumes knowledge of Windows scripting. Retrospect's external scripting functionality is only for experienced script authors who wish to further automate Retrospect with external scripts. If you want to learn Windows scripting, start with Microsoft's web-based documentation for developers.

Due to the complex nature of Windows scripting, Tqzkq offers only minimal support for these features.

Installing Windows Scripting Support Files for Retrospect

The External Scripts folder is installed by the Retrospect setup program in default ("Recommended") installations. You can add it to your Retrospect folder by using the setup program to modify the existing installation.

When you install Retrospect, the External Scripts folder, by default, is installed here:

..\Program Files\Retrospect\Retrospect 7.5\ External Scripts

Windows Script Host must be installed on your system to use scripts created with VBScript or other scripting languages not directly supported by the operating system. Windows Script Host is available free from Microsoft.

Retrospect Events

Retrospect has fifteen events that can be handled by scripts. Retrospect client software has two of these events. Below are the event names and descriptions of when they are triggered.

StartApp occurs when Retrospect is opening, including when it is autolaunching.

EndApp occurs when Retrospect quits.

StartBackupServer occurs when Proactive Backup is about to start.

StopBackupServer occurs when Proactive Backup is stopped.

StartScript occurs when a script is about to start.

EndScript occurs when a script is finished.

StartSource occurs when a source is about to be accessed for the first time. This event is present in both the Retrospect application and Retrospect client software.

EndSource occurs when a source has finished being accessed. This event is present in both the Retrospect application and Retrospect client software.

MediaRequest occurs when Retrospect is about to request media, and again every five minutes while the media request window is open.

TimedOutMediaRequest occurs when Retrospect has requested media and it has waited longer than the time specified in the preferences.

ScriptCheckFailed occurs when Retrospect quits after running a script and there is a scheduled script set to run outside the look ahead time and the script check fails.

NextExec occurs when Retrospect quits after running a script and there is a scheduled script set to run outside the look ahead time and the script check passes.

SchedStop occurs when a script is running and about to stop because its allowed time of execution has expired.

PasswordEntry occurs after someone enters a password.

FatalBackupError occurs when a fatal backup error occurs.

Implementing a Script with Retrospect

Copy your external script file to the Retrospect program folder (the default path is ..\Program Files\Retrospect\Retrospect 7.5) and rename your script RetroEventHandler. Add the filename extension that matches your script type, such as .BAT, .EXE, .VBS, or any other supported by Windows Scripting Host.

NOTE: If more than one RetroEventHandler file is present, only one will be used. If you want to take multiple actions with multiple events, you must write a single script to do it.

Implementing a Script with a Retrospect Client for Windows

To use external scripting with a Retrospect client, copy your script file to the Retrospect Client program folder (the default path is ..\Program Files\Retrospect\Retrospect Client) and rename it as detailed in "Implementing a Script with Retrospect".

Executing an External Script

When an event occurs, Retrospect notifies the external script and waits for a response from the script before continuing. After five seconds, Retrospect displays a status window to indicate it is executing a script.
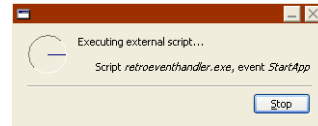
When the script finishes, Retrospect continues.

Sample Scripts

The External Scripts folder includes sample scripts written in four script languages (batch files, Visual Basic, VBScript, and C). You can study the source code of an example in a given language to learn how to write your own script to handle Retrospect events. They demonstrate how you might use the information sent for each event and provide examples of the acceptable values returned.

To use an example script with Retrospect, copy it from its sample folder to the Retrospect program folder.

NOTE: The .BAT batch example script uses the batch command extension ask.exe, installed in the Retrospect program folder.

The example scripts display a window as each event occurs, naming the event and listing the event's information. For example, opening Retrospect triggers the StartApp event.
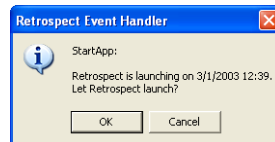
You must respond in each window to allow Retrospect to continue. You must do something else to trigger another event that will be handled by the example script.

After sampling an example script, remove it from the Retrospect program folder so it doesn't interfere with your backups or other scheduled Retrospect scripts.

Useful Scripts

The External Scripts folder includes some working scripts you may find useful. To use one of these, copy it from its folder to the Retrospect program folder.

Lotus Domino Server Application

This external script is designed to back up a Lotus Domino Server running as an Application. This batch file requires the Microsoft Windows Resource Kit to be loaded. Using this script, Retrospect will quit the Lotus Domino Server, perform a consistency check, compress its databases, then back up.

When Retrospect completes its operations, the Lotus Domino Server application will be restarted.

This batch file requires the user to configure the path to the Domino Server directory (for example C:\Lotus\Domino) and set the version number of the Domino Server (for example, 4.6a=460, 5.0.2=502). These settings are in the top portion of the batch file and are clearly noted.

Lotus Domino Server Service

This external script is designed to back up a Lotus Domino Server running as a service. Using this script, Retrospect will stop the Lotus Domino Server service before backing up. After Retrospect finishes backing up, the Lotus Domino Server service will be restarted.

This batch file requires the user to set the name of the service to match the name of Lotus Domino Server service in the services control panel (for example, Lotus Domino Server). The name of the service will differ for different versions of Domino.

PROBLEMS AND SOLUTIONS

- **TROUBLESHOOTING**

- **COMMON QUESTIONS**

- **RETROSPECT ERROR MESSAGES**

- **RETROSPECT ERROR NUMBERS**

- **RETROSPECT CLIENT ERRORS**

- **RETROSPECT SUPPORT**

This section offers solutions to problems you may encounter with Retrospect and its clients. It includes general troubleshooting help, answers frequently asked questions, and introduces you to the same troubleshooting techniques Tqzkq Retrospect Technical Support uses to solve problems.

"Troubleshooting" includes common problems encountered during installation and backup and restore operations and offers explanations and solutions. "Common Questions" presents frequently asked questions. These questions do not involve error messages and are more general than the troubleshooting problems. "Retrospect Error Messages" provides a numerically ordered list of error numbers with detailed explanations. "Retrospect Support" offers troubleshooting techniques and procedures for getting help.

TROUBLESHOOTING

Most problems encountered while using Retrospect fall into a few general categories. Tqzkq Retrospect Technical Support follows some basic troubleshooting procedures for each of these categories. With a little effort, you can learn how to troubleshoot many problems on your own. This section outlines those procedures and shows you the most common problems and their treatments.

TIP: The first thing you should do when you encounter an error is to make sure that your version of Retrospect is up-to-date. Choose Retrospect Updates from the Help menu, then click Check Now to check for available updates to your current version of Retrospect. Install the latest updates to see if they resolve your problem.

We recommend that you keep notes of your troubleshooting efforts. Even if you are unable to resolve a problem right away, your notes can establish a pattern of behavior to help us both understand the problem. If, after reading this section, you find you are still unable to solve a problem, try using some of the other Retrospect support resources. See "Retrospect Support" on page 346.

Troubleshooting Road Map

The first step in troubleshooting a problem is to isolate the problem by identifying exactly when and where it occurs. Knowing when an error occurs gives you a fixed point of reference to help you solve a problem. Retrospect has different phases of operation. For example, a backup typically includes scanning, matching, copying, and verification phases in that order. If you can determine the problem happens while matching, you are on your way toward solving it.

Client Configuration Issues

A client in the local subnet or in another Retrospect-configured subnet does not appear in Retrospect's live network window, or appears intermittently.

Use the Test button in the live network window to see if the client is on the network.

Open the Retrospect Client control panel on the client computer and check whether the client software was loaded at startup and whether it is turned on. Check that its status field says "Ready" or "Waiting for first access." If it is a Mac OS client check that it is actually a TCP/IP client and that it does not say "AppleTalk" next to its version number.

Make sure the client computer is connected to the network and its network settings are correct.

Should these measures not work, see "Testing and Pinging to Verify TCP/IP Communication" on page 322. If the backup computer and client ping successfully yet the client still does not appear, your network may not fully support TCP/IP and UDP. Passive networking hardware, such as hubs and bridges, may not forward network information Retrospect needs to work with TCP/IP clients. Retrospect's advanced networking lets you directly add a client by its DNS name, WINS name, or IP Address (see page 179) and may skirt around the problems and let you work with a client.

After taking the appropriate measure you may log in the client.

If the client has more than one Ethernet card, that might also be the source of the problem. See "Troubleshooting multiple ethernet cards on a Retrospect Client running Windows" in the Tqzkq Retrospect Knowledgebase (www.tgvtqur gev.com/knowledgebase) for more information.

A client outside the local subnet does not appear in Retrospect's live network window.

The live network window shows only clients Retrospect found in a specific network with a specific way of searching for clients.

Retrospect Professional can only access clients connected to the backup computer's local subnet. Retrospect Single Server, Multi Server, and Small Business Server can access clients directly anywhere on the network by using an IP address, DNS name, or WINS name. It can also access clients on any network segment you define. See "Advanced Networking" on page 179.

If the client has more than one Ethernet card or NIC, that might also be the source of the problem. See "Troubleshooting multiple ethernet cards on a Retrospect Client running Windows" in the Tqzkq Retrospect Knowledgebase (www.tgvtqurgev.com/knowledgebase) for more information.

See also "–530 (backup client not found)" on page 338 and "–541 (backup client not installed or not running)" on page 338.

The advanced networking direct access method fails to connect with the client at the specified IP address or name.

Make sure the client computer is connected to the network and its network settings are correct.

Open the Retrospect Client control panel on the client computer and check whether the client software was loaded at startup and whether it is turned on. Check that its status field says "Ready" or "Waiting for first access."

Make sure the IP address you are using is current. If the client is using dynamic IP addressing its IP address may have changed. It is not a good idea to directly add a dynamic address unless it has a long-term lease. Use the subnet broadcast access method instead.

If you are using the client's DNS or WINS name try using its IP address.

Ping the computers to check whether they are correctly communicating with TCP/IP. See "Testing and Pinging to Verify TCP/IP Communication" on page 322.

There may be a firewall between the client's network and the backup computer's network, restricting outside access. For example, Windows XP with Service Pack 2 enables the firewall by default. See the Tqzkq Retrospect Knowledgebase (www.tgvtqurgev.com/knowledgebase) for information on creating a firewall exception for Retrospect and Retrospect Client.

The advanced networking direct access method added the wrong client.

Make sure the IP address you are using is current. If the client is using dynamic IP addressing (for example, DHCP) its IP address may have changed. Use the subnet broadcast access method instead. Also see "Common Questions" on page 323.

Backup Issues

Immediate backups and scripted backups differ in the way they are started and what they do when they are done. Otherwise, both follow the same procedure after starting: scanning, matching, requesting media, copying, comparing, and then closing.

Retrospect fails to automatically launch to execute a scheduled script.

There are a few reasons why this can happen:

- **Confusion About Start Date**: The date you expect a script to run may not be its actual start date. See "Common Scheduler Elements" on page 135.

- **Incorrectly Scheduled Script**: Check the list of future scripted operations to confirm that Retrospect has the same schedule you

expect your scripts to run. To do this, click Activity Monitor>Scheduled. Check that you have not set a limited schedule of possible execution times with the Schedule preference (see page 264).

- **Autolaunch Preference Not On**: Check that the unattended execution preference is turned on (see "Startup Preferences" on page 266).

Retrospect crashes while it is being launched.

The Config75.dat file may be damaged. Move it (and any other configuration files, "config**.***") out of its parent folder and try launching again. If this solves the problem, place the suspect configuration file in the recycle bin. (Retrospect creates a new configuration file using the default settings.) If you do not want to recreate your scripts and settings and log in clients again, you can rename the Config75.bak file to Config75.dat, or restore a recent version of the Config75.dat file from a backup.

The Config75.dat and Config75.bak files can be found either in the same folder as the Retrospect application, or in ../Documents and Settings/All Users/Application Data/Retrospect.

Windows NT reports a registry quota alert.

Take the following steps to increase the registry size.

1. Open the System control panel.

2. Click the Performance tab.

3. Click the Change button for Virtual Memory.

4. Change the maximum registry size to something higher, typically double the current value.

Retrospect reports an error during scanning or matching.

There may be a problem with the volume being scanned. In this case, Retrospect reports a specific error in the Operations Log.

Look up the error number in "Retrospect Error Messages," which starts on page 332.

A removable cartridge drive does not appear in the Volumes Database or media request window.

Removable disks (such as Zip, Jaz, SuperDisk, DVD-RAM, or MO) must be accessible with a drive letter in the Windows Explorer.

A tape drive or CD/DVD drive does not appear in the Storage Devices window or media request window.

Go to Configure>Devices and click the Environment tab. If the driver name listed for your device does not appear in boldface, some other software loaded a driver inappropriately, keeping Retrospect from using its own driver. Determine which other device driver is loading and disable it.

All devices should be connected before launching Retrospect. Verify the drive is properly connected and terminated then make sure it is turned on. If other devices on the communications bus are off, turn them on and restart. Use Retrospect's Environment tab (from Configure>Devices) to review your ID settings. For a SCSI device verify it has a unique SCSI ID number.

Under Windows 98/Me, make sure ASPI is installed. Run the ASPI check utility from the Retrospect folder. If it reports ASPI is not fully installed on your computer, run the ASPI installer from the Retrospect folder. See "ASPI" on page 32 for more information.

On Windows NT, 2000, and XP systems, Retrospect uses NT Passthrough by default to access devices. When using ASPI instead, if the

ATAPI miniport driver is disabled Retrospect will not see the ATAPI bus. You must enable the miniport driver by editing the registry key at the path:

```
\\HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\Aspi32\
Parameters
```

Set the ExcludeMiniports value data to empty so Retrospect sees all buses.

If you have a new drive model, it may not be supported by the version of Retrospect you are using. To find out if a newer version of Retrospect is required for this drive, refer to the Tqzkq Retrospect web site.

Retrospect reports "the drive can't be used because no drive letter is assigned" for a CD/DVD drive that has an assigned drive letter.

Under Windows NT, 2000, or XP if the ATAPI miniport driver is disabled Retrospect reports the drive does not have an assigned drive letter.

You must enable the miniport driver by editing the registry key at the path:

```
\\HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\Aspi32\
Parameters
```

Set the ExcludeMiniports value data to empty so Retrospect sees all buses.

Retrospect can't use the inserted disk or tape because it is "busy."

There are several possible causes.

- You saved the disk Backup Set Catalog on a disk that is a Backup Set member. Catalogs must be saved on different volumes. Move the Catalog to your hard disk and double-click it to force Retrospect to recognize it.

- You are using the disk as both a source and destination, which is illogical and not allowed. For example, you are trying to back up the 2-Dunsinane volume to the Dunsinane Backup Set, of which 2-Dunsinane is a member.

- Some other software may be creating or using files (which may be invisible) on your backup disk. Likely suspects are compression programs; see the latest "read me" file for conflicts and workarounds.

- The drive may be malfunctioning. Contact the drive vendor for assistance.

- The medium may be damaged. Designate it as missing and use a new medium.

Retrospect refuses to use the inserted medium.

Retrospect has a system for recognizing media and for adding them to Backup Sets. If Retrospect is not automatically using the tape or disk you think it should, carefully read the text that appears in the media request window. It explains what medium Retrospect needs.

You may not have inserted the exact medium required by Retrospect. Check that the name of the medium you are inserting exactly matches the requested name. If the name is the same and Retrospect does not proceed with the operation when you insert the medium, you probably have two pieces of media with the same name and are inserting the wrong one. This can happen if you switch media when you perform a Recycle backup to a particular Backup Set.

TIP: Turn on the "Automatically reuse named media" preference to avoid this scenario. See "Erasure Preference" on page 268.

Retrospect may require new media. Insert the tape or disc you want Retrospect to use and wait for it to appear in the window, or click Add to use hard disk storage space, and then click Proceed. Retrospect will not use media that is part of a known Backup Set, as detailed below. It will automatically use any media that is erased or correctly named.

Retrospect asks for a new medium, but then complains "You can't use '1-Birnam Wood', it already belongs to a Backup Set!"

This is a feature designed to prevent accidental erasure. If you are sure you want to erase this medium and use it for the current backup, click Erase from the toolbar, then click Proceed if necessary. Erasing the medium removes the entry for this member from the Backup Set it previously belonged to.

Retrospect asks for a particular medium, but then reports '"2-Dunsinane' is not a member of this Backup Set. Although it is named correctly, it has a different creation date."

This means you have more than one medium with the same name. This can happen if you run a Recycle backup to new media and later try to do a Normal backup with older media. If possible, locate the proper tape, disk, or CD/DVD for the restore.

Try other media to see if any match the Catalog you are using.

If you are sure this medium has the files you want, rebuild its Catalog. Click Tools>Repair Catalog, and select the appropriate repair function to recreate the Catalog. See "Recreating a Catalog" on page 302.

Retrospect asks for a particular medium, but you do not have it.

If you know where it is, but it is not available right now and you must back up, follow these instructions. Click Choices, then click Skip. Retrospect treats the requested member as if it were full and backs up progressively to a new piece of media. Files previously backed up to the requested member are not backed up again. Future backups will require the new member and you will need to use both members later if you need to restore.

Once you click Skip, you will not be able to take advantage of the remaining free space (if any) on the skipped member.

If you know it is lost, damaged, or erased, follow these instructions. If this is the first member of the Backup Set, it is easiest to start a new Backup Set or run a Recycle backup to this Backup Set. Either way, Retrospect asks for a new medium, which becomes the new first Backup Set member. If this is not the first member and you wish to continue backing up progressively to the members you do have, click the Choices button, then click Missing. Retrospect will start backing up to a new medium. Files that were backed up to the missing member will be backed up again, if possible, during your next Progressive Backup.

Retrospect reports a Catalog out of sync error at start of backup.

Update your Catalog from the media.

See "Updating a Catalog" on page 301.

Retrospect reports a chunk checksum error.

If the error occurs only with a particular Backup Set, repair its Catalog and try again.

See "Updating a Catalog" on page 301.

Retrospect reports verification errors.

Retrospect reports different kinds of errors depending on the type of verification you are using.

Thorough verification compares the files on the destination media to the files on the source. If Retrospect reports "different modify date/time…" for a particular file, the most likely explanation is that the file was modified during the backup. In this case, no action is required. When you next back up, Retrospect will re-copy the file.

Errors such as "File … didn't compare at offset…" usually indicate a problem with the communications bus (for example, SCSI or ATAPI). Back up again to re-copy the file.

Note, however, that these "offset" error messages usually point to serious data corruption problems you should not ignore. If the error occurs with many or all sources, including clients, or with a source connected to the backup computer itself, troubleshoot its communications bus. If the error occurs only on a particular source being backed up over the network, troubleshoot the communications bus of that computer and possibly the network connection to that computer.

See "FireWire and USB Device Issues" on page 320, "SCSI Issues" on page 321, and "Network Troubleshooting Techniques" on page 322. Consider using diagnostic software on affected volumes.

Media verification compares MD5 digests for the files on the destination media to MD5 digests generated when copying the files from the source.

When Retrospect reports that these MD5 digests do not match, this usually indicates a problem with the destination media (e.g., the media is corrupt, or data was written to a bad disk sector). Check your Backup Set media for problems. If you cannot correct the problems, you should back up to new media. Files that generate Media verification errors, by definition, do not match those in the destination Backup Set. Therefore, they will be recopied to the destination during the next backup.

NOTE: In certain circumstances, Retrospect does not have access to MD5 digests generated during backup. This is true for all backups created using versions of Retrospect prior to Retrospect 7.5, as well as backups that took place when Retrospect's "Generate MD5

digests during backup operations" preference was disabled. See "Verification Preferences" on page 270 for more information. In these cases, Retrospect still checks all files on the Backup Set media to make sure that they are readable.

When it has finished executing an operation, Retrospect does not quit, log off, restart, or shut down according to the Unattended preference.

Retrospect quits, logs off, restarts, or shuts down when it finishes only if it is executing an operation in unattended mode and no additional operations are scheduled within the look ahead period (see page 264).

Retrospect automatically enters interactive mode when you start an immediate operation and unattended mode when you start a script. While Retrospect is copying, use the Control menu to switch between modes.

A Macintosh client does not shut down after the backup.

Retrospect shuts down Macintosh client computers when all four of the following conditions are met.

• The client is running Mac OS 9.x or prior.

• The Shutdown when done option is enabled in the client options of your script (this is the default).

• The client is displaying the "waiting for backup" dialog.

• The client is not scheduled for another backup within the look ahead time (see page 264).

Retrospect is not backing up a particular client volume.

Check that your backup script includes the volume as a source.

Make sure the client volume is not designated as private (see page 185).

Make sure the client's volume is mounted for use with the client computer. (Under Mac OS, the volume icon is on the Desktop; under Windows, the drive letter is accessible.)

Use the client container as the source, rather than specific client volumes, to select all volumes connected to the client. Then go to Configure>Clients, get the properties of the client in question, click the properties window's Volumes tab, and choose Client Desktop from the list box.

For more information about using client containers see "Configuring Clients" on page 173.

The client crashes during the backup.

Failing network hardware, a virus, or a software conflict may be causing the client to crash. Use diagnostic utilities to look for viruses and hard disk problems. If it is a Mac OS 9.x or prior client, refer to the system extensions troubleshooting techniques in "Troubleshooting Mac OS Clients" on page 323. Use the latest network software which matches your network hardware.

Proactive Backup Issues

Proactive Backup indicates "media," but there is a medium in the drive.

Proactive Backup is reporting it needs a specific media member to back up a source. To determine which Backup Set needs more media, click the Backup Sets tab in the Proactive Backup status window and look for any Backup Set with a status showing "media."

If you have never backed up to the Backup Set that needs media, Retrospect accepts any new or erased medium. Stop Proactive Backup, use Configure>Devices to erase the medium you want to use, then start Proactive Backup again.

If you still cannot determine why Proactive Backup is not accepting your medium, start a backup to that Backup Set using Backup>

Backup. Retrospect displays a window naming the medium being requested.

Retrospect does not quit when Proactive Backup completes its backups.

Proactive Backup is optimized to run continuously. If you have other kinds of scripts, they will start at their scheduled times even though Proactive Backup is still running.

If you schedule Proactive Backup to run only part of the time (for example, from 7:00 A.M. until 7:00 P.M. each day), you can quit Retrospect after the Stop time without affecting Proactive Backup. Retrospect will automatically launch when the next script is scheduled to start.

The Retrospect Client control panel's Proactive Backup Schedule was set to "As soon as possible" but the client was not immediately backed up.

The "As soon as possible" preference waits for Proactive Backup to poll the client; the client does not initiate contact itself. Meanwhile, Proactive Backup may be busy backing up other sources or polling other clients; it may even be inactive, according to its schedule. When Retrospect does poll the client set to ASAP, it backs it up.

See "Allow Early Backups" on page 144.

Restore Issues

When you start a restore, you first select the Backup Set from which you are restoring. Retrospect then goes through the following stages: selecting a volume (specifying where the files are going), matching or selecting files, requesting media, copying, and setting privileges if necessary.

You have problems selecting a Backup Set.

If your Backup Set is not in the list, click the More button. Click Open if the Catalog for your

Backup Set is available, or click Recreate to rebuild it from the media.

If Retrospect reports a chunk checksum error after selecting a Backup Set, see "–641 (chunk checksum didn't match)" on page 339.

You have a medium that you want to restore from, but you do not see its Backup Set in the selection window.

Use Windows Explorer to look for the Backup Set Catalog File on your hard drive. It will have the same name as the medium in Retrospect's Storage Devices window. For example, if a tape is named "1-Macduff" look for a Catalog File named "Macduff". Double-click the Catalog File to show Retrospect where it is.

If you cannot find the Catalog File on your hard drive, click Tools>Repair Catalog, and select the appropriate function to recreate it (see page 302).

You cannot find the files you want to restore.

If you are using "restore selected files," be sure the Snapshot you select is for the right volume. By default, the files chosen preview browser shows your files and folders in alphabetical order, organized as they were on the backed-up hard disk. Once you find the file you want, double-click it to mark it for retrieval. If you cannot find your file, choose Find from the Edit menu to search by name or other attributes. A file with a poof icon indicates the file is on a missing member of the Backup Set.

If you are restoring older versions of files, use Restore>Find Files. Tell Retrospect to look for a particular file or folder name, and if necessary click More Choices to use Retrospect's Selector interface for finding files.

See "Restore" on page 69 and "Using Selectors" on page 291.

While retrieving an older Snapshot from media, Retrospect says no Snapshot is available.

There are two possible causes:

- You turned off the "Save source Snapshots for restore" option (see page 241).
- You cancelled the backup before it was completed. Retrospect does not save a Snapshot for a volume until the backup is finished.

Retrospect refuses to use the inserted medium, reporting it is named correctly but has a different creation date.

This means that you have more than one medium with the same name. This can happen if you run a Recycle backup to new media and then try to restore with older tapes, disks, or CD/DVDs. If possible, locate the proper medium for the restore.

Try other media to see if any match the Catalog you are using.

If you are sure this medium has the files you want, rebuild its Catalog. Click Tools>Repair Catalog, and select the appropriate repair function to recreate the Catalog. (See "Recreating a Catalog" on page 302).

Retrospect reports the disk is full while copying during restore.

The volume you are restoring to does not have enough space for the files you are restoring. You will need to manage your disk space by moving or deleting files, or avoid the problem by marking fewer files to restore. If you are restoring a volume that was using a compression utility, you may need to restore your files in batches and use your compression utility between restores to make room for the next batch of files.

After restoring, NTFS security permissions are not set.

You must restore by Snapshot and leave on the option to copy security information. See "Windows Security Options" on page 245 and "Restoring from a Full Backup" on page 207.

After restoring, Mac OS file sharing privileges are not set.

Retrospect will only set the privileges for Mac OS 9 file sharing while sharing is active. (Note that sharing also had to be on during backup.) Turn on sharing and restore again.

Before restoring to a volume other than the current system volume under Mac OS X, use the Finder's Show Info command on the volume. Choose Privileges from the info window's menu then turn off the "Ignore privileges on this volume" option.

See "Restoring Mac OS File Servers" on page 215.

After restoring a Macintosh OS 9.x or prior client, documents have generic icons in the Finder.

The Macintosh Desktop needs to be updated after a large restore. Restart the Macintosh while holding down the Command and Option keys to rebuild the Desktop.

After restoring a backup to a new Macintosh hard disk, the volume icon on the Finder Desktop is no longer custom. It is now generic.

Restart the computer.

After restoring, Subvolume definitions for a Macintosh client are wrong.

Subvolume definitions may be re-identified following an operation restoring a large number of folders. The Subvolumes may have incorrect names (because they were re-associated with incorrect folders) in Retrospect's volume selection window and browsers. The cause has to do with the invisible directory identification numbers of folders.

To prevent this rare problem from occurring, erase or format the destination volume before you use Retrospect's "restore entire volume" feature. To avoid Subvolume confusion, check the names and accuracy of all Subvolumes after any large restore operation (such as restoring an entire disk). You will have to re-define each Subvolume on a volume after a full volume restore.

You can't retrieve or restore data to a client.

Take the following steps:

1. Attempt to access the client. From the client database, select the client and click Properties from the toolbar. Click the Refresh button to check whether Retrospect can connect to the client.

2. Go to Configure>Volumes, select the volume to which you wish to restore data, and click Properties from the toolbar. Make sure the volume has enough free space to accommodate the files you want to restore, and that there is no lock symbol on the Attributes line. (If there is no Attributes line it is not locked.)

If you are sure that the volume to which you are restoring data is both unlocked and has free space but you still experience difficulty restoring, refer to Chapter 8 • Disaster Recovery for general assistance.

User Initiated Restore Issues

UIR has a number of requirements in order to function correctly. Make sure to review the requirements described throughout "User Initiated Restore" on page 191 first. If both your Retrospect backup server and Retrospect Clients meet the requirements for UIR and are set up correctly but users still cannot access the UIR web page, there are several things you can try:

• Make sure IIS is running on the backup computer.

- Run the ASP.NET IIS Registration tool. Enter the following text at the Command Prompt on the Retrospect backup server to correct the problem: `C:\WINDOWS\Microsoft.NET\Framework\v1.1.4322\aspnet_regiis.exe -i` If the path to "aspnet_regiis.exe" is different than the one is listed above, make sure to enter the correct path.
- Try to connect to the UIR web page from the Retrospect backup server. If you can connect from the backup server, but not from Retrospect Clients, there may be issues with your network that are blocking access. Contact your network administrator to find a solution.

If users can access UIR, but cannot complete a restore, there a number of error messages that display in the UIR web page and provide information about how to solve the problem:

- *User Initiated Restore is not turned on.* Turn on User Initiated Restore. Open Retrospect and choose Configure>Preferences from Retrospect's navigation bar. Choose Clients>User Restore and select the "Enable User Initiated Restore" check box.
- *Could not connect to Retrospect.* Launch Retrospect on the backup server.
- *Retrospect was unable to find a client on your machine*. Make sure a supported Retrospect Client is installed on your computer and is turned on.
- *A Retrospect client was found at IP address _____, but is not logged into the Retrospect server*. From the Retrospect backup server, add the Retrospect Client into the Backup Clients Database. See "Adding Clients" on page 171 for more information.
- *The Retrospect Client at IP address _____ is turned off*. From the Retrospect Client computer, turn the client on. See "Client User Preferences" on page 183 for more information.
- *The Retrospect Client at IP address _____ is set to read-only access*. From the Retrospect Client computer, make sure the client is set up to provide full access. See "Access Restrictions Preferences" on page 185 for more information.
- *The Retrospect Client at IP address _____ is currently in use.* Wait and try to connect again later.
- *No backups for _____ were found*. Make sure you are backing up the Retrospect Client. If it has never been backed up, UIR has nothing from which to restore. This error could also display if a new Retrospect Client gets installed on a user's computer. If a user with a new Retrospect Client wants to have access to her old backups, the Retrospect backup administrator needs to reassociate the old client (and its backups) with the new client. Choose Configure>Clients from Retrospect's navigation bar. In the Backup Clients Database, select the old client name and click Properties. Click the Access tab, then click Change. Select the new client name or enter the client address and click OK.

Finally, users may be able to access UIR and restore files, but the files they want to restore may not be available through UIR. UIR only displays the active Snapshots for each backed up volume. In general, that means that only the most recent backups are available for restore.

In most cases, it is probably best and easiest for the administrator to perform an immediate restore from within Retrospect when a Retrospect Client user needs to restore files older than those available in UIR. There are ways to make older Snapshots available, but they require some action on the part of the administrator:

- Retrieve older Snapshots. When you use Retrospect to retrieve older Snapshots from the backup media, those Snapshots become active and thus become available in UIR. For information about retrieving Snapshots, see "The Snapshots tab" on page 257.

- Change the disk Backup Set's grooming policy to retain more backups. If you increase the number of backups to keep before grooming, there will be more Snapshots available in UIR. However, this requires additional disk space to store the older backups.

FireWire and USB Device Issues

If you're having problems with FireWire or USB devices it could be due to a number of issues.

Hardware Issues

- Isolate the device. Another device on the chain may be interfering with the backup device's communication. If your backup device is connected to your computer through a hub or another FireWire/USB device, unplug it and connect it directly to a port on the computer. If it is already connected directly to the computer, try changing ports. If the problem persists, do not reconnect the other devices, and continue down the checklist.

- You may have a bad cable. Replace the cable that connects the device to the computer.

- The system board or FireWire/USB adapter in the computer may be having a problem. Install Retrospect on another computer, if available, and try the device there as the only device.

Media Issues

- Try a new piece of media to see if the problem is related to a faulty or damaged medium. If applicable, try using a different brand of media. Often drives are picky regarding the brand of media. Follow the manufacturer's recommended list of brands.

- If you are using a tape drive, clean the heads with a cleaning cartridge.

Windows 98 Issues

- Microsoft has made dramatic improvements to USB and FireWire (1394) support with Windows 98 Second Edition. If you are experiencing media failures, communication errors or other device problems during backup, consider upgrading your version of Windows 98. Windows 98 Service Pack 1 is better then the original Windows 98. SP 1 is a free upgrade from Microsoft. Windows 98 Second Edition is better then Service Pack 1 but is a paid upgrade from Microsoft.

- We also recommend installing the Windows 98 Second Edition 1394 Storage Supplement, available from, www.microsoft.com.

- Turn off auto insert notification in CD-RW device manager properties.

Firmware/Software Issues

- Check to make sure you have the latest USB or FireWire firmware update for your computer. Hardware vendors often release firmware updates that may help to resolve USB or FireWire issues. Search the vendor web site for Updates. Retrospect lists the current firmware of the drive that you are using in the version column of the Device Status (or Environment) window. If there is a known problem with a firmware version, this will be listed on the Tqzkq Retrospect web site.

- Update or reinstall the FireWire and USB adapter drivers. Corrupt drivers can cause issues that may not be otherwise detectable. Check the manufacturer's or vendor's web site for updated drivers.

- Completely uninstall any other third-party backup software that may be on your machine, including any drivers that software may have loaded for the device.

If you have investigated all the issues listed about and still get failures on new media, then the backup device itself may be defective. Contact your drive vendor for further diagnostics, tests, or to inquire about repair or replacement.

SCSI Issues

If the SCSI chain is not set up properly, communication errors may cause data corruption or system failures during copy operations. The following information is designed to give you guidance when you encounter SCSI problems.

Also see "USB/USB 2.0" on page 31, your SCSI card's user's guide, and the manual that came with your hardware device.

These sample errors can indicate communication errors on a SCSI bus:

- File "Tech Note" didn't compare at offset 3,253
- Trouble reading: "1-Office Backup 2" (0), error –102 (trouble communicating)
- Trouble writing: "1-Macbeth" (0), error –205 (lost access to storage medium)

These errors can usually be traced to a failure in the SCSI configuration, whether it is termination, a particular device, cabling, or device order. The most common cause of SCSI bus communication problems is improper termination or bad SCSI cables. Try changing terminators, using a powered terminator, changing cables, isolating the device on the SCSI chain, and moving the device to a different computer. If it is a tape drive, clean its heads and if cleaning does not work, try different kinds of tapes.

Termination

The general rule for termination is to use only two terminators on the SCSI bus; one at the beginning and one at the end. If you have only a single device on the SCSI bus, then only one terminator is needed because your SCSI card should have built-in termination. Some SCSI peripherals come with internal termination built in, and must be placed at the end of a SCSI chain.

Consult your hardware's user guide for its specific termination requirements.

SCSI Cables

Communication problems can be caused by bad or loose-fitting SCSI cables. Check all cables to ensure they are properly seated in each connector. The entire length of your SCSI bus should not exceed 20 feet. Whenever possible, try to use short (12 to 36 inches) cables and avoid cables over six feet in length.

Device Order and Device Conflicts

To avoid problems caused by device order or device conflicts, make sure that each device has a unique SCSI address. To see the SCSI address of every device, click Configure>Devices. Then click the Environment tab to view all of your devices. You may print this window for future reference. If problems occur (for example, a device does not appear that you know is turned on and connected), try changing the order of SCSI devices or temporarily removing unneeded devices. Recheck that each device has a unique SCSI ID.

Some devices, such as scanners and removable disk drives, can cause communication failures on the SCSI bus, especially if they are turned off. If you are experiencing SCSI communication problems, make sure all of your SCSI devices are turned on when you use your computer. Even if you are not experiencing SCSI problems, we highly recommend you turn on all SCSI peripherals before starting the computer.

Do not turn them off until after you shut down the computer.

Unresolved SCSI Problems

If everything is properly set on the SCSI chain, there is still the unpredictability of "SCSI voodoo," the cause of problems which theoretically should not occur because the "rules" of SCSI are being followed. SCSI voodoo may require you to rearrange the devices on the chain, change the termination, assign new IDs, or replace SCSI cables. (Short cables cause less problems than long ones.) In theory SCSI has well-defined rules and expected results, but in practice SCSI sometimes is an inexact science.

Network Troubleshooting Techniques

Testing and Pinging to Verify TCP/IP Communication

Use the Test button in the live network window to see if Retrospect can connect to a computer on the network via TCP/IP and communicate with the client software. Click Test and enter an IP address, DNS name, or WINS name. If Retrospect reports error –541, it connected to the computer at that address but no client software responded. If it reports error –530, Retrospect could not even connect to the computer. Other errors may indicate network and TCP/IP configuration trouble and you should "ping" the backup computer and client computer from other computers to check whether they are communicating with TCP/IP.

Windows computers configured for TCP/IP have built-in ping commands. From a TCP/IP Windows computer on your network, go to the MS-DOS command prompt and type "ping" followed by a space and the IP address.

Mac OS 9.x and prior does not include a ping utility, but you can obtain a ping-capable utility from the Internet. Such utilities include iNetTools (www.wildpackets.com), IPNetMonitor (www.sustworks.com), Interarchy (www.interarchy.com), OTTool

(www.neon.com), and WhatRoute (homepages.ihug.co.nz/~bryanc).

On Mac OS X, click the Ping tab on the Network Utility (located in /Applications/Utilities).

NOTE: TCP/IP must be loaded when you ping a Mac OS 9 computer. To ensure it is loaded, open the TCP/IP control panel, uncheck the option "Load only when needed" (available only in Advanced and Administrator modes) and restart.

Using an IP pinging utility on the troublesome client computer, first ping the IP address of the backup computer. A reply tells you the pinged computer's TCP/IP setup is operational. If it times out or reports it as unreachable there is a problem with the TCP/IP setup, the network interface hardware, or the network itself.

If pinging the backup computer is successful, use it or another computer to ping the IP address of the troublesome client computer.

Selecting the Appropriate Network Driver

The backup computer and Windows client computers should be using 32-bit network drivers for best network performance and compatibility. Windows NT, 2000, and XP use 32-bit network drivers by default. For Windows 95/98/Me, open the Network control panel and select the computer's network interface adapter. Click the Properties button, select Enhanced mode, and click OK. You may need to get updated software from your network adapter vendor.

Verifying Open Transport Version

To work with TCP/IP, Mac OS 9.x and prior clients must have Open Transport version 1.1 or later. Each computer's TCP/IP control panel should be set to always load, as described previously.

NOTE: Mac OS X clients do not require Open transport.

Troubleshooting Networks

When you have network problems with Retrospect or clients, start by identifying a pattern of failure. If the problem occurs on a single client, begin your troubleshooting by examining that particular computer. If the problem occurs on multiple client computers, find out if those computers share a common hub, router, bridge, or gateway. You may be able to identify a faulty network component that should be repaired or replaced. If you encounter failures on multiple client computers but cannot identify a pattern, troubleshoot the networking hardware on the backup computer.

Troubleshooting Mac OS Clients

When troubleshooting an individual Macintosh, the first step is to determine whether the problem lies with the Macintosh's software or its network hardware. The following information describes how to troubleshoot Mac OS 9.x and prior clients.

For detailed information on troubleshooting Mac OS X clients, read "I can't see an OS X client on my network. What can I do?" in the Tqzkq Retrospect Knowledgebase. From within Retrospect, choose Online Knowledgebase from Retrospect's Help menu.

Start by limiting extensions and control panels on the client Macintosh to the Retrospect Client control panel, needed networking software, and minimal default Apple system software. Do this with the Extensions Manager.

If the client continues to experience the problem, there may be an incompatibility with networking software. If the client has a third party networking card, update to the latest version of its software. If the client uses its built-in Ethernet, get the latest version of Apple's network software installer or Open Transport, available from the Apple Software Update web site.

If the client continues to experience the problem, exchange the network hardware with that of another client Macintosh. Whether it uses built-in Ethernet or an Ethernet adapter card, it is sufficient to exchange all components external to the Macintosh. If the Macintosh has an internal network card, you will need to exchange the card as well. Make sure to exchange the cables along with the other components. After exchanging the network hardware, try an operation with both clients. If the error moves to the other client, then the problem lies in the network hardware.

If the problems persist after minimizing extensions and exchanging network hardware, performing a clean installation of the System software.

COMMON QUESTIONS

This section answers common questions about setting up and configuring Retrospect Clients, backing up files locally and over the network, Backup Sets, Catalogs, devices, and media.

Client Setup Questions

How do I find out the IP address of a client so I can access it directly?

It depends on the operating system and how the client computer is configured. If the client has a static IP address you can use it with the direct access method. However, if the client automatically obtains a dynamic IP address from a DHCP server you probably should not be using the direct access method. Dynamic IP addresses may change later and Retrospect may find a different machine at that address if you directly added a dynamic IP address. You should use multicast or subnet broadcast instead.

Here's how to determine a computer's IP address and whether it is static or dynamic.

Mac OS: Open the TCP/IP control panel (OS 9.x or prior) or Network preferences (Mac OS X) on the client. It shows the "IP Address" the computer is currently using. Above the IP address is the Configure pop-up menu. If it shows "Using DHCP Server" it is a dynamic address. If it shows "manually" it is a static address.

Windows 95/98/Me: From the Run dialog or the DOS prompt, enter WinIPcfg, which shows some configuration information in a window. Click its More Info button to see the full configuration.

Windows NT/2000/XP: Open the DOS prompt and enter "IPconfig -All", which lists the full IP configuration.

All Windows Systems: The IP configuration information shows the IP address the computer is currently using. It shows whether the computer is using a DHCP server and, if so, shows the lease dates of the automatically obtained IP address. If it does not show DHCP server and lease information, the IP address was specified manually (that is, it is static).

Client Configuration Questions

How do I change the name of a client?

The client is named when it is first accessed from the backup computer.

If a client has already been logged in and you want to change its name, click Configure> Clients, double-click the client to be renamed, then click the Tools tab in the client properties window. Click the Rename button and enter a new name.

The name change will not affect previously backed up files—they are still stored under the old client name. New files and Snapshots will be stored under the new name.

How do I log in a client when I forgot its password?

You must uninstall the client software, reboot the client computer, then reinstall the client software with a new password.

How can I get back a client volume after accidentally using Forget?

If you forget a client's volume, you can put it back into Retrospect's volume lists by configuring the client (see page 173). Remember to add the volume to the appropriate scripts, if necessary.

Backup Questions

How do I back up to a hard disk drive?

Use a disk Backup Set or a file Backup Set on the hard disk. See "Backup Sets and Their Components" on page 23 and "Hard Disk Drives" on page 37.

How do I back up a Snap Server or other NAS? How do I use it as a backup device?

Retrospect works with Network Attached Storage (NAS) devices in a number of ways. You can run the Retrospect application or Retrospect Client on the NAS device, or you can use the NAS device as the destination to store data for file and disk Backup Sets.

See "Network Attached Storage (NAS) Devices" on page 50 for more information.

How do I back up only files which have changed?

Retrospect does this automatically. The first time you back up, Retrospect copies all selected files. On subsequent Normal backups, it copies only the selected files which are new or changed.

How do I specify complete (full) or progressive (incremental or differential) backups?

By default, Retrospect does progressive backups; i.e. it backs up only new or changed files. You can modify this behavior by setting the

backup action. See "Backup Actions" on page 24 for more information.

There are many ways to do this:

- When executing an immediate backup, by changing the backup options (see page 237).
- When running a script by selecting an item from the manual execution dialog's combo box (see page 139).
- When creating a script scheduler (see page 135).
- By configuring the Backup Set and clicking the Media Action button see (page 256).

How do I back up multiple volumes to the same tape, disk, or CD/DVD?

Use the same destination Backup Set. To back them up at the same time, select each volume you want to back up in the volume selection window. You can make a non-contiguous selection using the Control key or select a range of volumes using the Shift key. When you execute the backup, Retrospect backs up each of the selected volumes, one after another.

You can later do Normal backups of other volumes to the same Backup Set and Retrospect will add them to the medium until it is filled.

How do I quickly start a backup?

First create a script in Retrospect and save a run document (see page 139) from it. Use the run document to start that script directly from the Windows Explorer.

How do I include or exclude files with particular attributes?

You can specify which files Retrospect backs up by using selectors. These allow you to include or exclude files by their size, kind, dates, and many other attributes. See "Using Selectors" on page 291.

Network Backup Questions

How do I see what was backed up last night? How can I tell if everyone has been backed up by Proactive Backup?

The Backup Report shows a summary of the backup operations for each volume. To view the report, click Reports>Backup Report. See page 229.

The Operations Log shows by date and time which volumes were backed up, how much data was copied, and whether the backup completed successfully. To view the log, click Reports> Operations Log. The log also lists any errors which occurred. See page 231.

To view files backed up during the most recent backup, click Reports>Session Contents. Select the appropriate Backup Set from the top list in the contents report window, select one or more sessions from the bottom list, and click Browse. A browser appears, listing the files in the order they were backed up. See page 233.

To see all files on a particular volume at the time of a given backup, get the Backup Set properties and view the Snapshots tab. See page 257.

Can more than one backup computer run on the same network at the same time?

Yes, you can run multiple backup computers at the same time on the same network with no problems, though when they transfer data at the same time both backups will probably slow. If you run backups in different physical network segments, traffic on one segment will not affect other segments.

I want to make a computer on a different network segment the backup computer. What should I do?

Moving to a new backup computer is explained in detail in "Moving Retrospect," which starts on page 272.

How can I use multiple network cards on the backup computer?

Retrospect Multi Server allows you to acess all clients from multiple subnets without crossing your network backbone. Connect each network interface card to a separate network segment and use Retrospect's advanced networking features (see page 179) to configure a separate interface for each card/subnet combination.

What is Retrospect's network port number?

Retrospect uses a well-known port, 497, assigned by the Internet Assigned Number Authority (IANA), for both TCP and UDP.

How many client computers can I back up from a single backup computer?

There is no fixed limit to the number of clients you can access from one backup computer. It is not a question of numbers, but more a question of resources. You can back up more clients with a faster backup computer, a faster backup device with higher capacity media, and simply more time to do the backups.

If the backup computer is not completing backups in its scheduled time periods or if you want volumes to be backed up more often than they are, you may need a faster backup computer or a faster backup device, if not both.

Why do my network backups take too long?

For a discussion of backup performance, including guidelines for estimating your backup speed, see "Network Backup Guidelines", and "Choosing the Backup Computer" on page 198.

If you notice that your backups have suddenly become much slower, or if one particular client backs up more slowly than others with a similar configuration, you may be experiencing a problem. Potential problems may lie with the following:

• **The amount of activity on the backup and client computers during the backup.** Other applications (anti-virus software for example) running on either computer draw processing power away from Retrospect. Try a backup with Retrospect as the only application running on the backup computer for optimal performance.

• **The amount of data being copied.** Recycle backups tend to show higher performance figures than Progressive Backups. For each backup, Retrospect must spend time examining the entire volume to determine which files need to be backed up, regardless of the amount of data that needs to be backed up. The ratio of this overhead time to total backup time will be higher for a small amount of data (Progressive Backup), as compared to a large amount of data (for a Recycle backup or when an empty Backup Set is first used in a Normal backup). Backups of small amounts of data may therefore report slower performance times than backups of large amounts.

Table 11-1 below shows sample data from several backups. Performance figures for the Recycle backup are much higher than for subsequent backups of the same client due to the lower proportion of overhead time to the amount of data actually backed up.

• **The total number of sessions for which a Backup Set has been used.** The greater the number of sessions created, the longer Retrospect takes to match sessions to determine what files need to be backed up. Periodically resetting your Backup Set with a Recycle backup or adding new media to your rotation using a New Backup Set backup will limit the number of sessions in your Backup Set, thereby speeding up both your backup and restore operations.

• **File sharing.** File sharing slows copying on both clients and the backup computer. Turning off file sharing when it is not needed can help optimize network performance.

• **Backing up across network segments.** The backup computer and a client may reside on two physically different networks connected by a bridge or router that may slow the progress of data from one machine to the other. Backup performance may also suffer if the two networks vary greatly in terms of their relative network activity or performance. You can confirm the speed of the connection between the backup computer and the client by getting properties

from Configure>Clients. If the echo time seems higher than under normal circumstances (for example, consistently above 0.3) or the KB/second performance figure seems lower than normal, a network problem may be affecting your backup speed. Get properties to view the performance figures for various client computers and compare them to determine current levels of network performance.

• **The performance of the backup and/or client computer.** Problems with either machine affect the speed of your backup. Specifically, you should check for hard drive fragmentation, problems on the SCSI bus, and network problems.

• **The speed of the backup computer.** Different computer models feature various central processing units with various clock rates (for instance, a relatively slow Pentium or a relatively fast Pentium III) that determine how quickly they perform tasks. The performance of similar CPUs also varies based on their clock cycles (as expressed in megahertz). Finally, the speed of the SCSI bus varies among the different expansion cards, influencing how fast each computer can transfer data across its SCSI bus. For optimal backup performance, assign a relatively fast computer to run Retrospect.

Backup Action (iteration)	Number of Files	Megabytes Copied	Time (mm:ss)	MB per minute
Initial Backup	8345	719.6	24:00	30
Progressive (1)	51	5.7 00:2	2	15.4
Progressive (2)	360	19.7	01:26	13.8
Progressive (3)	43	5.7	00:25	13.5
Progressive (4)	53	6.1	00:30	12.6

Table 11-1: Sample values for client backups over an Ethernet network.

• Using encryption or software compression.
If possible, avoid using encryption on the backup media or link encryption for client computers. Encryption requires additional processing power the backup computer would otherwise use to increase backup performance. Whenever possible, use hardware compression (if your tape drive includes hardware compression capabilities), since hardware compression works faster than software compression. Because backup speed influences tape capacity, hardware compression also allows more data to fit on a tape.

How do I determine a working speed threshold for the client execution option?

Get the properties of several different clients from the clients database window. For about a minute, observe the speed of each client.

Can Retrospect shut down a Windows client computer when it is done with its backup?

No. The Retrospect client software for Windows does not support software shutdown because most PCs must be turned off with a hardware switch.

Can I duplicate the system from one Windows computer to another?

No, because too much of a Windows computer's information is specific to that computer. Each card, peripheral, and software program requires specific settings which are unlikely to carry over from one PC to another, even if they were identical models and configurations.

Do I have to upgrade my clients to the latest version?

Tqzkq strongly recommends using the latest version of the Retrospect client software with clients used with the latest version of Retrospect.

How can I prevent the "waiting for backup" dialog from appearing on Macintosh

clients on nights when no operation is scheduled?

The Retrospect Client control panel has no way of knowing when an operation is scheduled to occur, so it always waits at shutdown if this option is turned on in the Retrospect Client control panel preferences dialog. There are several ways to get around this if you do not perform operations every night.

Make a script using the No Files selector then schedule it to run on nights when no backups are scheduled. Retrospect shuts down the script's Macintosh sources.

Tell users which days they should click the Shut Down button in the "waiting for backup" dialog when they leave for the day.

Turn off the Wait at Shutdown preference in the Retrospect Client control panel on each user's Macintosh. Tell the users which nights to leave their Macintosh computers on. Remind them to turn down the monitor brightness or turn off its power to prevent screen burn-in.

Will Retrospect wake a sleeping PowerBook Mac OS client to back it up?

Retrospect cannot wake a PowerBook in sleep mode, but a PowerBook will not go to sleep while it is plugged in and AppleTalk is on.

Restore Questions

I thought I just restored some files. Where are they? Where did they go?

Look on the root level of your hard disk for a folder with the same name as the Backup Set from which you restored.

Does Retrospect restore empty folders?

Yes. Empty folders are restored when you restore from a Snapshot using Restore>Entire Volume, using any option except "Restore just files".

I backed up multiple volumes using a single backup script. How do I restore all of the volumes at once?

Create and schedule a restore script for the first Snapshot you wish to restore. Duplicate this script. Edit the copy of the first script, changing the source and destination to reflect the next Snapshot to restore. Repeat this process for each volume you wish to restore. Retrospect runs each script, one after the other, alphabetically by script name, starting at the time you specified.

Backup Set and Catalog Questions

What if I forget my Catalog?

If you forget a Backup Set Catalog from within Retrospect, its file remains on your hard disk until you drag it to the recycle bin. If you have mistakenly told Retrospect to forget a Catalog, you can open the Catalog File from within Retrospect or from Windows Explorer. After forgetting a Catalog, you must add the Backup Set to your scripts again because Retrospect removes them when you forget the Catalog.

What if I lose my Catalog?

If you lose your Backup Set Catalog (perhaps because it was deleted, corrupted, or lost), you can have Retrospect recreate the Catalog by scanning last member of the Backup Set. See "Recreating a Catalog" on page 302.

If the Fast Catalog File Rebuild option was turned off, Retrospect will need to scan all members of the Backup Set. If this is the case, it may take several hours to recreate a Catalog if there is a large amount of data in the Backup Set.

Can I delete files from a Backup Set?

No, you cannot delete files from a Backup Set because most types of storage devices do not allow it. If you want to keep only selected files from a Backup Set, you can copy these files to a different Backup Set using Retrospect's Backup

Set transfer operation. See "Transfer Backup Sets" on page 90.

Can I rename a Backup Set?

Retrospect has no facility for renaming Backup Sets but you can rename a file Backup Set in the Windows Explorer. (Other types of Backup Sets cannot be renamed.) Open the file Backup Set after you rename it to make Retrospect recognize the change.

Can I put more than one Backup Set on a tape, disk, or CD/DVD?

You cannot have more than one Backup Set on a tape or CD/DVD but you can have multiple file Backup Sets or disk Backup Sets on a disk. When you add a removable medium to a Backup Set, Retrospect reserves the entire medium for that Backup Set.

You can, however, back up as many volumes as you want to a single Backup Set.

What is the best way to manage Catalog Files?

Catalogs typically contain about 4 MB for each 10,000 files you back up. Keep your often-used Catalogs on your hard disk. If you have little available space on your hard disk, here are a few alternatives:

• Store infrequently used Catalogs on a file server.
• Archive old Catalogs to their own Backup Set.
• Compress the Catalogs. See "Configuring Backup Sets" on page 255.

It's a good idea to duplicate Catalog Files in case they are damaged.

I back up by moving a tape drive from computer to computer. What is the best way to do this?

It is not necessary to create a separate Backup Set for each computer unless you plan to use a different tape for each workstation. If you use a

single Backup Set for the computers, do not do a Recycle backup of each workstation; use Normal backup only, and New Backup Set backup when you need to rotate media.

After each backup, copy your Backup Set Catalog to a server or removable disk and then, once you move to the next computer, copy the Catalog to its hard disk. You may want to use Retrospect's Catalog compression option (see page 256) to keep the Catalog as small as possible.

Alternatively, keep the Catalog on a server accessible from each computer. This, though, assumes all of your computers are connected by a network, in which case you will save yourself a great deal of trouble by purchasing Retrospect Clients. For less than thirty dollars per client, Retrospect client software allows Retrospect to back up Windows and Mac OS computers over a network without moving the backup device.

What are the consequences of not saving Snapshots to save time and space?

Turning off the Save source Snapshots for restore option (see page 241) mainly makes it harder to view or restore a volume's folder hierarchy.

Without a Snapshot, you cannot:

- restore a volume to its exact state as of a given backup, as you would after a crash, for example;
- restore the Windows registry (necessary when restoring an entire disk);
- restore NTFS security information;
- restore empty folders;
- browse a volume backup for restoring.

Should you need to restore files, you will have to use a selector (and/or browse "flat files" without hierarchy) to choose which files to restore—a time-consuming process.

Devices and Media Questions

Why are my DAT tapes filling up sooner than I expected?

Drives using the DDS-1 format support 60 or 90 meter tapes for an uncompressed data capacity of about 1.3 GB or 1.9 GB, respectively. Drives using the DDS-2 format support 120 meter tapes for an uncompressed data capacity of about 4 GB. Drives using the DDS-3 format support 125 meter tapes for an uncompressed data capacity of about 12 GB. Drives using the DDS-4 format support 150 meter tapes for an uncompressed data capacity of about 20 GB.

For typical everyday use, when your tape is full, it may store up to 30% less data than its ideal maximum capacity.

If you use a drive with hardware compression, you can effectively increase the capacity of your tapes. Your tape's actual capacity will depend largely upon how well the data you are copying compresses. Text compresses well, for example, but applications do not.

If you back up many small files or back up files over a network, your tape's actual capacity will also decrease.

Retrospect requests a new tape for one of three reasons:

- The tape drive reports the current tape is full.
- An error occurred while writing to the tape. Open the log to see if an error occurred.
- You selected Skip or Missing while configuring a Backup Set, or you are performing a New Backup Set backup.

How much space is left on my tape?

Retrospect estimates your tape's capacity to help you manage your backup. To view this estimate, click Configure>Backup Sets. In the Backup Set selection window, select your Backup Set and click Properties. The window

that appears lists the estimated available space on that Backup Set's current member.

This estimate is only to help you gauge when Retrospect will request new media. Regardless of the estimated available space, Retrospect uses a member until the tape drive reports the tape is full.

Because many tape drives do not report a tape's capacity dynamically, Retrospect's estimate may be inaccurate. To change the estimate to match your tape's actual capacity (based on your own experience), uses the Capacity button as described in "The Options tab," which starts on page 256.

What do I do when I know my tape or disk is going to fill up during tonight's backup?

If you think there is not enough space for the next backup on the current tape or disk of your Backup Set, you can tell Retrospect to ask for a new one.

To skip to a new member, use the Media Action button, described in "The Options tab," which starts on page 256. The next time Retrospect adds files to that Backup Set it will ask for new media, in effect skipping over the blank space at the end of the current member.

If this situation arises frequently, consider using Retrospect's Automatic skip to blank media preference. When this preference is on, Retrospect automatically uses any erased media if the current member is not available.

You might also consider purchasing a tape library, a backup device which holds a magazine of many tapes. When one tape fills, Retrospect uses an empty tape from the magazine.

When I try to erase a tape or disk Retrospect asks for the Catalog File, but I no longer have it. How can I erase the tape?

When you erase a disk or tape, Retrospect tries to remove the member's contents from the Cat-

alog for that Backup Set. If it is missing, Retrospect asks you for it. You need to tell Retrospect to forget the Catalog because it is gone, which will then allow you to erase the tape. Go to Configure>Backup Sets and Forget the Backup Set then go to Configure>Devices and Erase your tape.

If I have two tape drives, will Retrospect use them both when performing unattended backups?

Yes it will if the devices are similar, with the same kind of mechanism. When it fills up a tape, Retrospect looks in any available drive for any tape that is new or erased, or has the correct name.

If you have Retrospect's Advanced Tape Support add-on, you can run simultaneous operations using both tape drives at once.

See "Multiple Concurrent Executions" on page 161 for more information.

How do I start over at the beginning of the tape?

Insert the tape and click Configure>Devices. The devices window that appears shows you the name of the tape. Select the tape and click Erase from the toolbar.

WARNING: Erasing a tape that is a member of a Backup Set erases the backed up files.

How do I recycle tapes from old Backup Sets?

To re-use a tape from a Backup Set that you no longer need, insert the tape, and click Configure>Devices. The Storage Devices window that appears shows you the name of the tape. Select the tape and click Erase from the toolbar. The next time Retrospect requests a new member for a Backup Set, it will automatically use this or any other erased tape in the backup device.

You should also remove the old Backup Set's Catalog. Click Configure>Backup Sets. In the

Backup Set selection window that appears, select the old Backup Set and click Forget from the toolbar. Drag the old Backup Set Catalog File to the recycle bin.

How do I determine the name of a certain tape?

To view the name of a tape, click Configure> Devices. Retrospect scans for available tape devices. The Storage Devices window appears, listing each tape drive, its status and location, and the name of the inserted tape. Insert the tape if you have not done so.

Once you know the name of a tape, use a soft-tip pen and the manufacturer's adhesive labels to identify the tape cartridge.

Can I use my audio DAT or DV camera deck for backup?

No.

Can I use audio DAT tapes in a DAT drive?

No. While audio-grade DAT tapes can be used in some computer DAT drives, we recommend data-grade media. Data-grade tapes must pass more stringent testing than audio-grade tapes. More recent computer DAT drives recognize only Media Recognition System (MRS) data-grade tapes.

Miscellaneous Questions

In summary windows and browsers, why do the file sizes reported by Retrospect differ from the Windows Explorer?

The discrepancy in size is due to the difference between any given file's logical size and its physical size. The logical size of a file is the actual number of bytes the file contains. The physical size is the amount of space the file occupies on a hard disk or other volume. This physical size varies for a given file depending upon where you store the file (for example, on a floppy disk or a hard disk). Retrospect reports a consistent size based on the physical size of a file, regardless of where you store the file.

How do I get rid of a Backup Set I don't need anymore?

Click Configure>Backup Sets. In the Backup Set selection window, select the Backup Set to be removed and click Forget from the toolbar. This removes the Backup Set from the destination lists of all your scripts. To remove a Backup Set completely, you must also drag the Backup Set's Catalog File to the recycle bin with Windows Explorer.

How do I get rid of a volume that no longer exists?

Click Configure>Volumes. In the volume selection window, select the volume to be removed and click Forget from the toolbar. This removes the volume from the source lists of all your scripts.

When I quit Retrospect, how can I prevent the message that tells me the next time Retrospect will execute?

Click Configure>Preferences. Select the Notification Alerts Preferences category and turn off Check validity of next script.

Where are my scripts stored?

Your Retrospect scripts are stored in the Config75.dat file. The Config75.dat and file can be found either in the same folder as the Retrospect application, or in ../Documents and Settings/All Users/Application Data/ Retrospect.

Many other customizations you make to Retrospect are stored there as well.

RETROSPECT ERROR MESSAGES

When Retrospect detects compare errors while backing up, write errors while retrieving, or read errors while retrieving or verifying, it opens a browser displaying the files involved. The execution errors browser may be printed for reference, or copied and pasted into another

browser for easy re-selection. Look in the Operations Log for the error message associated with each file and act appropriately.

When Retrospect is performing operations over the network, either the client or the backup computer can generate errors, which are then reported by Retrospect on the backup computer. In general, errors that are reported at the client occur when the Retrospect client software surveys the system and determines that Retrospect will not be able to use it over the network.

Catalog out of sync

Retrospect was unable to update the Catalog the last time it copied data to this Backup Set.

This may have been due to equipment failure or power failure, or was caused by a full disk or by a lack of memory.

If updating the Catalog does not eliminate the "Catalog out of sync" error Retrospect cannot add files to that tape. You have three options:

• Perform a Recycle backup, which resets the Catalog and erases the media, removing its existing backup files.

• Skip to a new member using the Media Action button (page 256), forcing Retrospect to use a new piece of media for the next backup.

• Create a new Backup Set and do a backup to new media.

Resynchronizing (slow)

When Retrospect reports this message during a Catalog update or a Backup Set recreation, the Backup Set medium in use may be damaged.

If this message appears for more than about fifteen minutes, stop the recataloging or recreation and save the partial session. You will not be able to add any more data to the medium. The next backup to this Backup Set will require a new or erased medium.

This error can indicate device communication problems. See "FireWire and USB Device Issues" on page 320, and "SCSI Issues" on page 321.

Bad Backup Set header

Retrospect encountered a missing or damaged file header, which contains information such as the file's name and size.

This error can indicate device communication problems. See "USB/USB 2.0" on page 31, and "SCSI Issues" on page 321.

Content Unrecognized

Retrospect can see data on the medium, but the data is not recognized as data formatted by Retrospect. With a removable cartridge, the unrecognized content most likely is other files, which you may not want to lose.

WARNING: When a floppy, Zip, Jaz, SuperDisk, DVD-RAM, or MO disk shows as Content Unrecognized, use caution. Any files on a disk are permanently removed when Retrospect uses the disk in an operation with a disk Backup Set.

For tapes this usually means that the tape was damaged, used by an incompatible backup program, or used with an incompatible drive. This often results with tapes used with hardware compression drives then used with drives which do not support the same hardware compression. Do the following to troubleshoot:

• Make sure the tape cartridge you are inserting is compatible with your tape drive. For example, DDS-4 150 meter tapes cannot be read by DDS-1, -2, or -3 drives. Refer to the Tqzkq Retrospect web site for current information on tapes that each tape drive supports.

• Clean your tape drive and continue to clean it according to your drive vendor's recommendations. Tape drives need to be

cleaned regularly with special cleaning cartridges (see page 42).

- Check if other tapes also show as content unrecognized. If only one tape does then either it is damaged, it has been written to by other backup software, or it was created in a different, incompatible tape drive. If all tapes are unrecognized, then they were either all created in a different tape drive, there is a problem with your SCSI configuration, or your tape drive may be broken. See "SCSI Issues" on page 321 for detailed instructions on troubleshooting your SCSI bus.

- If possible, try your tape or tapes in a compatible tape drive. If tapes are recognized in one drive but not another of the same type, it is possible that one drive needs repair. Contact your drive vendor for advice before assuming a drive needs repair.

Media too different

Retrospect reports that your media is too different in two cases:

- You are trying to append to a tape Backup Set that is damaged. If you crashed or experienced a power failure while last writing to your tape and are now getting this error when trying to append, your Backup Set is damaged. You will not be able to append to this Backup Set, but you can retrieve all files from it. Create a new set, or do a Recycle backup to this set if you wish to start over. The media is not damaged, but the Backup Set is damaged such that Retrospect cannot append to it.

- You are trying to append to a tape Backup Set using a drive with a different kind of mechanism. Use similar drives when creating mixed drive Backup Sets.

Verification Errors

The following messages indicate an error while comparing to verify files with Thorough verification:

- File "Home.html": different modify date/time
- File "Bore Dimensions": didn't compare at offset 263,078

Thorough verification errors occur when Retrospect determines a file it copied to the destination is not identical to the file copied from the source. The file in question is not considered valid in the destination. If this happened during a backup, for example, Retrospect would try to copy the file again during the next Normal backup to this Backup Set.

When you know the file was in use at the time the copying was done, a verification error is usually nothing to worry about. It simply means the file changed between backup and verification. Verification errors that mention offsets usually indicate problems with the communications bus. See "SCSI Issues" on page 321.

Media verification errors occur when Retrospect finds that the MD5 digests for the files on the destination media do not match the MD5 digests generated when copying the files from the source.

This usually indicates a problem with the destination media (e.g., the media is corrupt, or data was written to a bad disk sector). Check your Backup Set media for problems. If you cannot correct the problems, you should back up to new media. Files that generate Media verification errors, by definition, do not match those in the destination Backup Set. Therefore, they will be recopied to the destination during the next backup.

NOTE: In certain circumstances, Retrospect does not have access to MD5 digests generated during backup. This is true for all backups

created using versions of Retrospect prior to Retrospect 7.5, as well as backups that took place when Retrospect's "Generate MD5 digests during backup operations" preference was disabled. See "Verification Preferences" on page 270 for more information. In these cases, Retrospect still checks all files on the Backup Set media to make sure that they are readable.

Media request timeout after waiting

This is how the Operations Log reports error –1204 (user didn't respond).

Failure Notification

Retrospect experienced a major problem not due to normal errors or circumstances. When this happens, Retrospect creates an error log in the Retrospect folder named "assert_log.utx".

If you experience one of these errors restart your computer and try to do what you were doing when the error occurred.

RETROSPECT ERROR NUMBERS

If Retrospect is unable to complete an operation, it will display an alert with an error number. This section explains some common error numbers in greater detail.

–102 (trouble communicating)

The backup computer lost contact with the backup device.

Check the communications bus and device cabling, termination, and settings. See "FireWire and USB Device Issues" on page 320 and "SCSI Issues" on page 321.

–107 (out of application memory)

Effectively the same as error –625.

–203 (hardware failure)

The backup device is having problems because of a bad medium, a communications problem, or a mechanical error.

If the error occurs only when you use a particular medium, that medium is probably damaged. Try using a new medium. If the error occurs when you use any medium, you may have a problem with your communications bus or device. Try turning off the backup device and computer for two minutes and then turning them back on again.

See "FireWire and USB Device Issues" on page 320 and "SCSI Issues" on page 321.

–204 (device busy)

This error will likely occur if you store the Catalog for a disk Backup Set on a disk used as a member of that Backup Set. Keep the Catalog on your hard disk.

–205 (lost access to storage media)

Usually indicates the communications bus was reset during a backup, causing Retrospect to lose contact with the medium.

This error usually indicates a communications bus problem and may be accompanied by an error –102 (trouble communicating). If error –102 accompanies error –205, see "FireWire and USB Device Issues" on page 320 and "SCSI Issues" on page 321.

If error –102 does not accompany error –205 and communication problems have been ruled out, the next step is to check for media failure on the source volume.

Some hard drives reset the bus when they sense they are experiencing a media failure. Try testing the hard drive with the software that was originally used to format it.

–206 (drive reported a failure, dirty heads, bad media, etc.)

There is trouble reading from or writing to the Backup Set medium. This error is always generated by the backup device, and is usually due to one of four causes.

- The media is physically defective and needs to be replaced. Try using a different medium.
- The heads on the tape drive are dirty and need to be cleaned. Consult the manual that came with your tape drive or contact the drive manufacturer for cleaning recommendations.
- Another device is causing interference. If you have a drive immediately next to another electronic device, try moving the devices further apart. Try removing one or more devices temporarily to see if there is some other device conflict. Try using your backup device on another computer to see if interference is caused by your monitor or other nearby electronic devices. Also see "FireWire and USB Device Issues" on page 320 and "SCSI Issues" on page 321.
- Retrospect can also report error –206 when a crash or power failure interrupts the backup computer or tape drive. Some tape drives require an end of data (EOD) marker on a tape to append data. If a tape does not have an EOD marker Retrospect may report error –206 when it next tries to append to the tape. Tape drives are responsible for writing EOD markers, but a drive may not get the chance if you shut down or restart the backup computer or the power is interrupted. Lacking an EOD, the tape will later produce error –206 when you try to append (write data) to it with Retrospect.

To avoid problems, take the following precautions: do not disable verification in scripts and immediate operations; let the tape drive fully rewind or eject the tape before you power off or restart the computer; and if the computer crashes, try to eject the tape (using the drive's eject button) before restarting or turning off the computer.

When Retrospect reports error –206 on a tape because it lacks an EOD marker, that tape is un-usable for future appends until you erase it, though it is not physically damaged and you can use it to restore. The tape cannot be repaired with Retrospect's repair tool. To use the tape for additional backups or archives, you must first either reset the tape's Backup Set from Configure>Backup Sets or erase the tape from Configure>Devices.

When the error persists on multiple media and you have eliminated the above possibilities, the device may be failing. Contact the vendor.

–503 (backup client turned off)
The client was turned off by the user at the client computer before the operation started. The Retrospect Client control panel will automatically turn on when that client is restarted.

–505 (backup client reserved)
The client is in use by another backup computer. A client may be used by only one backup computer at a time.

This can also happen when the backup computer or client computer crash during an operation. Restart both computers.

–507 (incorrect password)
Make sure you are properly typing the password. It is case sensitive, so you must type the password's proper upper case and lower case letters. Make sure you are entering the *password* for the client, not a *license code.*

If you cannot remember the password for a client, you must uninstall the Retrospect Client software, reboot the client computer, and then reinstall the client software with a new password.

–508 (access terminated)
The client user has turned off the Retrospect Client control panel during the operation. When this occurs, the backup computer logs the error and moves on to the next client.

–515 (piton protocol violation)

Retrospect sees its data is becoming corrupt while being transferred over the network. It is usually caused by a hardware failure.

Look for a pattern to these errors. If the problem occurs only on one client, it is likely that there is a problem with the client's network connector or its connection to the network. If the problem happens on several clients with no coherent pattern, the problem may be with the backup computer's network card or connection, or with a gateway/router common to all network transactions. See page 322 for more information.

–519 (network communication failed)

The backup and client computers ceased to communicate, a situation which has many causes and solutions, as detailed below.

A user shuts down a client during the backup, or the client fails or is disconnected from the network during a backup. Determine why the client is failing or what part of the network communication link is failing (for example, a router, bridge, hub, or individual network connector). See the next item for help in determining if the problem is due to a software conflict.

A user is using too many applications on the client during the backup, or an application takes up most of the computer's processing power. Schedule backups for periods when the client is idle.

A network communication problem caused by hardware or software is making transactions unreliable. A failed network connector on a client will cause errors on that client. To determine whether a failed network connector is causing the problem, try switching connectors with a nearby computer that is not experiencing problems. See "Network Troubleshooting Techniques" on page 322.

A bad or failing hard disk is hanging the client computer. If the hard disk read light on the cli-

ent is stuck "on," and not blinking, and the client must be restarted before it will work, the client has a failing hard disk or a bug in the hard disk's firmware or software. For the hard disk that is hanging, update its driver to the latest version from its vendor. Then try running a disk-checking program.

Your network software is incompatible with your network hardware. Use the latest network software which matches your network hardware because older software might have problems.

Windows: Two different bugs in Windows 95 can cause the client to lose contact with Retrospect. Make sure the TCP/IP fix and Winsock 2.0 have been installed on Windows 95 clients. See "Working with Windows Clients" on page 188 for details.

Mac OS: An extension or some other software on the Macintosh has broken the network connection. Make sure you are not using software applications which prevent communication, such as older versions of security or compression programs that are active during a backup. Try starting up the Macintosh with the Retrospect Client control panel turned on, but all non-Apple extensions turned off.

This error may be caused by a problem with built-in Ethernet on all non-G3 PC I-based Mac OS computers. It tends to occur during large data transfers on a busy network. One solution is to upgrade to Mac OS 8.6, which has a new extension that fixes the problem. Another solution is to install and use third-party Ethernet cards. For more information, use the knowledgebase on the Tqzkq Retrospect web site to search for "PCI networking."

–525 (name/login conflict)

Usually this error appears when a client has been uninstalled and re-installed or replaced by client software which is not logged in.

On the backup computer, go to Configure>
Clients, select the client experiencing the problem, then Forget the client. Click Add to go to
the live network window and add the client of
the same name. Add the client to your scripts.

–527 (backup client was renamed)

Another backup administrator has renamed a
client from another backup computer. Simply
configure the client again to update the namein
your own client database.

–530 (backup client not found)

Retrospect cannot find the client computer on
the network. Make sure the client computer is
connected to the network and turned on and that
it is not powered off by energy saving software.
If it is a mobile computer make sure it has not
been "suspended" or put into "sleep" mode.
(Restart a suspended Windows computer to let
Retrospect see it.) Make sure the client has the
most recent version of the Retrospect client
software and that the client software loads at
startup.

If not, follow the suggestions provided for the
error "Client service not loaded at system start-
up" on page 342 or "Retrospect Client not
loaded at system startup" on page 344.

Test the connection between the backup com-
puter and the client by using Properties from
Configure>Volumes. If it can connect with the
client, Retrospect displays its measured transfer
rate in kilobytes per second. Also, try pinging it
(see "Testing and Pinging to Verify TCP/IP
Communication" on page 322).

If this error occurs with a Windows 95 client it
may be caused by a bug in the operating system.
Microsoft's Winsock 2.0 update fixes the prob-
lem. It is available free from Microsoft at:
http://www.microsoft.com/windows95/
downloads/contents/wuadmintools/
s_wunetworkingtools/w95sockets2/default.asp

–540 (trouble creating service)

Retrospect could not properly access a Win-
dows client. The error usually occurs with
Windows 95 clients that do not have Winsock
2.0 installed. Retrospect requires Winsock 2.0
to back up Windows 95 clients.

If the client already has Winsock 2.0 installed
under Windows 95, or it is running a different
Windows operating system, a required DLL or
system component on the client may not be in-
stalled. Reinstall the client software.

–541 (backup client not installed or not running)

The backup computer can see the client com-
puter at the IP address but no client software is
operational.

Make sure the client computer is turned on and
that it is not powered off by energy saving soft-
ware. If it is a mobile computer make sure it has
not been "suspended" or put into "sleep" mode.
Restart it and try again.

Open the Retrospect Client control panel and
examine its Status field for an error message
about why the client software is not working.
You may need to reinstall the client software.

If the backup computer has more than one
Ethernet card, that might also be the source of
the problem. See "Troubleshooting multiple
ethernet cards on a Retrospect Client running
Windows" in the Tqzkq Retrospect Knowledge-
base (www.tgvtqur gev.com/knowledgebase) for
more information.

–594 (lost communication with server)

This error occurs when Retrospect's "Automat-
ically check for available updates" preference is
enabled and Retrospect loses its connection to
the updates server while it is downloading an
update.

–625 (not enough memory)

There is not enough memory available to Retrospect for it to continue the operation. This error occurs most often when scanning volumes and Catalogs.

Retrospect may report this error when other applications are using most of the memory or your computer does not have enough RAM installed.

Try exiting your other applications, restarting, or adding more virtual memory swap space to make more memory available to Retrospect. Repeat the operation which brought about the error.

If your edition of Retrospect is capable of running multiple simultaneous executions, Tqzkq recommends the following:

- 2 execution units, 512 MB RAM
- 4 execution units, 1 GB RAM
- 8 execution units, 2 GB RAM

If you are following these guidelines and still encountering error -625, try reducing the number of execution units. See "General Preferences" on page 264.

–641 (chunk checksum didn't match)

One of Retrospect's files, likely a Catalog, is corrupt.

To check whether a Catalog is corrupt, set up a restore by searching on a blank file name so Retrospect scans all files in the Catalog. If the error occurs, you know this Catalog is corrupt.

If the error occurs during a backup or archive, you need to rebuild the Catalog (see page 302) of the destination. After the Catalog is reconstructed, reselect this Backup Set in your scripts. If the error occurs when you launch Retrospect, see "Retrospect crashes while it is being launched." on page 312.

– 843 (resource is in use by another operation)

The resource (volume, subvolume, Backup Set, etc.) you are trying to access is currently in use. For example, if you are trying to browse your C: drive while a subvolume of C: is being backed up.

Wait until the required resource becomes available and try again.

–1004 (database backup/restore error)

The database API reported an error.

In the operations log, the lines immediately preceding this error explain specifically what the API reported to Retrospect.

–1017 (insufficient permissions)

This error indicates that Retrospect was not able to access a volume during the backup operation.

This can happen when doing a scripted backup of a volume via Microsoft networking rather than a Retrospect Client.

Permission errors can occur under the following conditions:

- When the script was created you were logged in as user *X*. At the time of backup you are logged in as user *Y* who does not have permission to connect to the source server.
- When the script was created you were logged in as user *X*. At the time of backup you are not logged in.

This error can also occur when backing up to or from mapped network drives. If you receive this error when running scripts that involve mapped network drives, it is because the Retrospect Launcher service (the service that allows Retrospect to auto launch) needs to be configured to log on to the drives as a user with the appropriate privileges.

See the Tqzkq Retrospect Knowledgebase (www.tgvtqurgev.com/knowledgebase) for information on how to avoid -1017 errors in all these situations.

–1020 (sharing violation)

The file cannot be accessed because it is in use.

Another application or the operating system may have the files open, preventing Retrospect from accessing them. Exit the application that owns the busy file.

It is possible this error was reported on insignificant files and you can just ignore it.

–1101 (file/directory not found)

Retrospect cannot find a file.

This usually means you or someone moved or deleted one or more files and folders while an operation was in progress.

If this error occurs because a Backup Set's Catalog File was moved and Retrospect asks you where it is, use the file selection dialog to navigate through files and folders and point out the new location of the Catalog to Retrospect.

Try backing up again. If this error continues to occur, run a disk checking utility to check for possible directory corruption.

–1102 (drive missing/unavailable)

Retrospect cannot find the drive.

This error occurs with Subvolumes when the folder has been moved or deleted.

–1110 (general i/o failure)

A media problem occurred on a source volume.

Try verifying your source volume using a disk utility or the formatting program that came with your hard drive. Use ScanDisk on a Windows computer. On a Macintosh, use Drive Setup's Test command and Disk First Aid.

–1111 (locked range conflict)

A file is open by another application or service, using a lock range, preventing Retrospect from backing it up.

Try stopping the application before starting backups and resuming it afterward. Consider using Retrospect's external scripting ability (see page 306) to automatically stop and resume the other application.

–1115 (disk full)

A volume has little or no available storage space.

There are three causes of this error:

- You are restoring or duplicating more files than will fit on the destination volume.
- Retrospect is updating a Backup Set Catalog and the volume on which it is saved runs out of room.
- You are backing up to a file Backup Set and the destination volume runs out of free space.

Go to the Windows Explorer and make more space on the full hard disk by removing unnecessary files and emptying the recycle bin. Try marking fewer files to restore or duplicate, or select a larger destination volume. Use Catalog compression (see page 256) to make your Catalogs use less space.

–1204 (user didn't respond)

Retrospect could not find a requested disk or tape before the media request timeout period elapsed.

Turn off the media request timeout preference (see page 270) so Retrospect waits indefinitely for the requested media.

–2241 (Catalog invalid/damaged)

Effectively the same as error –641.

–2247 (snapshot not found)

Retrospect could not find the requested Snap-shot on the medium. For more information, see page 317.

–3047 (disk inactivity threshold not met)

You may see this error when using the Open File backup add-on. Open File Backup requires a period of inactivity on the source volume's disk (disk inactivity threshold) in order to accu-rately copy open files. The disk inactivity threshold is the amount of time Retrospect waits for the source disk to be idle in order to proceed with Open File Backup. When the threshold is reached, Retrospect waits again until the retry timeout occurs. The default threshold is 5000 milliseconds.

First, try reducing the threshold to a smaller number. See "Windows Open Files Options" on page 247.

For other suggestions, see "Open File Backup Tips" on page 276.

RETROSPECT CLIENT ERRORS

When backing up clients, you can also get error message on the client side. The errors appear in the client control panel on the client computer.

NOTE: Since NetWare clients do not have a control panel, no errors are reported to the client. Check the Operations Log for NetWare client issues.

Windows Client Control Panel Errors

When everything is set up normally and no errors have occurred, the control panel's Status tab should say "Ready" or "Waiting for first access" in the Status field. Below the status is the History area with information about the most recent operation or error messages.

Client service not loaded at system startup

If the status shows this error message, examine the history field for one of the messages from Table 11-2 below, then proceed as indicated.

There are a few possible reasons (in addition to those in the table) why the client software may not load at startup.

- The client software files are not in their proper location. The client software must be in the location you specified during the installation. Put it back in place or run the Setup program to reinstall the software. Log

in as the administrator or another user with full access privileges when you install.

- The client's service was terminated. This is unusual. You may be able to run Retroclient.exe to get the service operating, but because you do not know what terminated the service in the first place, it is best to restart the client computer.

Message	Action/Comment
Retrospect Client startup error: Winsock initialization failed.	There is a problem with the Winsock network interface. The file WINSOCK.DLL or WSOCK32.DLL may be an incorrect version (e.g., a non-standard Winsock). Re-install the DLL from the Microsoft Windows installation media.
Retrospect Client startup error: Protocol initialization failed. Make sure protocol is working.	Make sure the computer is using a valid IP address.
Retrospect Client startup error: Initialization failed. Make sure IP protocol is installed.	Install the TCP/IP network protocol from the Microsoft Windows installation media.

Table 11-2: Windows client control panel startup errors.

UNIX Client Control Panel Errors

When everything is set up normally and no errors have occurred, the control panel's Status tab should say "Ready" or "Waiting for first access" in the Status field. Below the status is the History area with information about the most recent operation or error messages.

Message	Action/Comment
"*JAVA_HOME* is set to an invalid location" *JAVA_HOME* represents the path to JAVA_HOME.	A symbolic link to /usr/bin/java does not exist or the JAVA_HOME variable in RetroClient.sh is not set to the correct location. Install Java if it is not installed. If Java is installed then follow the steps below. The RetroClient.sh file assumes that there is a symbolic link to the Java executable from the /usr/bin/folder. If this link does not exist, there are two ways of correcting the problem: 1) Create it: su to root cd /usr/bin ln –s /usr/jdk1.3/bin/java java Make sure that "/usr/jdk1.3/bin/java" reflects the path to the java executable where it was installed on your machine. 2) Change the line "JAVA_HOME=/usr/bin" to point at the "bin" folder of your Java installation folder.
"Either *RETROSPECT_HOME* or *DISPLAY* is not set!" *RETROSPECT_HOME* represents the path to RETROSPECT_HOME. *DISPLAY* represents the DISPLAY value.	During installation, RETROSPECT_HOME should have been set to the location of the installation, typically /usr/local/dantz/client. If this is defined and exported in /etc/profile then the user can just load the file with "./etc/profile" from the terminal where they want to start the Client Control Panel.
"Critical file missing."	Critical files missing from RETROSPECT_HOME path (either retrocpl or retrospect.jar). If these files have been moved, move them back to the RETROSPECT_HOME path. If these files are not present, reinstall the client.
"Error obtaining network status."	Indicates that the client is not running. The Client Control Panel cannot display client information until the client is started. Start the client.

Table 11-3: UNIX client control panel errors.

Mac OS Client Control Panel Errors

When everything is set up normally, and no errors have occurred, the Retrospect Client control panel should say "Ready" or "Waiting for first access" in the Status field. Below the status is the History area with information about the most recent operation or error messages.

Retrospect Client not loaded at system startup

If the message "Retrospect Client not loaded at system startup" is followed by one of the explanations in Table 11-4 below, proceed as indicated.

If this message appears by itself in the Status area, there are several possible causes.

- The Retrospect Client control panel file is not in its proper location. Place it in the Control Panels folder within the System Folder.

- You have not restarted the client after installing the Retrospect client software. Restart the client.

- You held down the Shift key when you restarted the client Macintosh, which prevented extensions from loading. Restart without holding down Shift.

- You have an extensions manager program that specifies that the Retrospect Client control panel not be loaded. Open the extensions manager and ensure the Retrospect Client control panel gets loaded at startup.

- Another control panel or system extension is conflicting with the Retrospect Client control panel. Test for a conflict by temporarily removing several system extensions and control panels from the System Folder, leaving the Retrospect Client control panel and standard Apple extensions then restarting the client Macintosh. After restarting, open the

Retrospect Client control panel. If you see the message "Ready" or "Waiting for first access," you know one of the items you removed prevented the Retrospect Client control panel from loading. You may avoid the conflict by making the Retrospect Client control panel load first on startup by replacing the ° symbol in its name with a space.

Message	Action/Comment
ROM or System Version too old	The Macintosh appears to be an antique, hopelessly incapable of running the modern networking software required for use as a client of Retrospect Backup for Windows. It is not even able to run the long-obsolete networking software required for use as a client of a ten-year-old version of Retrospect for Macintosh.
AppleTalk version too old	The Macintosh is trying to use AppleTalk, not TCP/IP. Verify that it meets the system requirements then install Open Transport and set up TCP/IP networking.
AppleTalk turned off	The Macintosh is trying to use AppleTalk, not TCP/IP. Verify that it meets the system requirements then install Open Transport and set up TCP/IP networking.
ADSP not installed	The Macintosh is trying to use AppleTalk, not TCP/IP. Verify that it meets the system requirements then install Open Transport and set up TCP/IP networking.
No Chooser Name specified	The Macintosh appears to be an antique, hopelessly incapable of running the modern networking software required to use it as a backup client with any Retrospect Backup edition for Windows. However, you can back it up with Retrospect for Macintosh.
No computer name or owner name specified in file sharing settings	For System 7.*x,* open the Sharing Setup control panel. For System 8 or later, open the File Sharing control panel. Enter computer and owner names then restart.
Network Name conflict: "Name"	Another client on the network is already installed with this Owner Name. Trash the Retrospect Client control panel and install a fresh copy.
Open Transport TCP/IP not installed	Install Open Transport and set up TCP/IP networking.
Mouse button held down	Holding down the mouse button during startup inactivates the control panel.
Doesn't run under A/UX	The Retrospect Client control panel cannot be used on a Macintosh running under A/UX.
Your activator code conflicts with John Doe (123.45.67.8). Please tell your backup administrator.	Forget one of the clients, trash its Retrospect Client control panel, then install Retrospect client software version 4.2 or later. Upgrade all older clients to prevent recurring errors.

Table 11-4: Mac OS client control panel startup errors.

RETROSPECT SUPPORT

Retrospect provides built-in access to a number of useful resources. From the Retrospect Help menu, you can access:

- **Online help contents page**. Fully-searchable and indexed guide to using Retrospect.

- **Retrospect Read Me**. Tips, late-breaking information, known issues, and workarounds.

- **Retrospect Updates**. Choose this option to check the Retrospect web site for free updates to your current version of Retrospect. See "Retrospect Updates" on page 15 for more information.

- **Tqzkq Retrospect Web Site**. Roxio Retrospect's home on the Internet. To access Roxio Retrospect's web site directly, go to www.retrospect.com.

- **Online Knowledgebase**. Searchable database containing answers to frequently asked questions about Retrospect-related terms, error messages, and troubleshooting techniques. To access the Knowledgebase directly go to www.retrospect.com/knowledgebase.

- **Supported Devices**. Searchable backup hardware compatibility database provides information of which devices Retrospect supports. To access supported devices information directly, go to www.retrospect.com/supporteddevices.

- **Roxio Retrospect Support**. Support section of the Roxio Retrospect web site. Includes links to tutorials, user forums, etc. To access the support section directly, go to www.retrospect.com/support.

All of these resources are available for free and can help you solve problems quickly and effectively to get the most out of Retrospect.

If you experience problems that you cannot solve using these resources, Roxio Retrospect Technical Support is available to help. To learn more about available support options, check Roxio Retrospect's support matrix at www.retrospect.com/support_matrix.

For information about contacting Technical Support in the U.S. and Canada, as well as internationally, see www.retrospect.com/contactsupport.

Log of Your Calls to Technical Support

Use the following form to keep track of calls to Roxio Retrospect Technical Support.

Registration Number:

Date	Technical Representative	Problem/Solution

SQL SERVER AGENT

- **REQUIREMENTS**

- **SECURITY**

- **INSTALLATION**

- **GENERAL USE**

- **BACKING UP**

- **DATABASE BACKUP HISTORY**

- **RESTORING**

- **DISASTER RECOVERY**

The SQL Server Agent provides the ability to back up and restore Microsoft SQL servers. Without the agent add-on, Retrospect cannot easily and reliably back up databases from a running SQL server.

You can back up a SQL server locally, running the Retrospect application on the server itself, or you can back up the SQL server as a Retrospect client, running the Retrospect application on a different computer.

REQUIREMENTS

There are different minimum requirements of Retrospect, SQL, and Windows, as described below.

SQL Server

The Retrospect SQL Server Agent works with the following combinations of operating system software and database software.

- SQL Server 2005, Windows Server 2003
- SQL Server 2005, Windows Small Business Server 2003
- SQL Server 2005, Windows 2000 Server
- SQL Server 2005, Windows 2000 Advanced Server
- SQL Server 2005 (64-bit), Windows Server 2003 (64-bit)
- SQL Server 2005 Express Edition (64-bit), Windows XP (64-bit)
- SQL Server 2000, Windows Server 2003
- SQL Server 2000, Windows 2000 Server
- SQL Server 2000, Windows NT 4.0 Server
- SQL Server 7, Windows 2000 Server
- SQL Server 7, Windows NT 4.0 Server

SQL Server Running Retrospect Application

To use a SQL server as the backup computer, running the Retrospect application on the server itself, one of the following application licenses is required:

- Retrospect Disk-to-Disk
- Retrospect Single Server
- Retrospect Small Business Server
- Retrospect Multi Server

You can upgrade the Retrospect application to a more powerful edition by entering a license code purchased from Roxio.

SQL Server as Retrospect Client

To back up a SQL server as a client, the backup computer must run Retrospect Multi Server (or Retrospect Disk-to-Disk, Small Business Server, or Single Server, with a server client) under one of the following operating systems:

- Windows NT 4.0
- Windows 2000
- Windows XP
- Windows Server 2003

SECURITY

If you will also be using the Retrospect Exchange Server Agent add-on, please read "Security" on page 360 for details on setting up Exchange Server Agent security.

Numerous security measures prevent an unauthorized user from simply launching Retrospect on the backup computer and backing up a SQL server. You must prepare Retrospect to run in the correct security context, or to access each SQL server in the correct security context. This involves configuring preferences in Retrospect so that the application runs as a certain user with sufficient privileges for the SQL server, or configuring Retrospect to log in to each SQL server individually using SQL authentication or domain authentication.

Regardless of whether you have yet installed or run Retrospect, and regardless of how you previously set its security preference, follow these instructions to ensure you can work with SQL.

Create and Manage User Logins

You must create a special login for use by Retrospect and identify human users of Retrospect as Backup Operators. These steps, which use Active Directory Users and Computers (Windows 2000 and 2003) or User Manager for Domains (Windows NT 4.0), are described below.

Create a Retrospect Backup User Account

Within the SQL server's domain, create a login dedicated for use by Retrospect, such as RBU (for Retrospect backup user account).

Make this account a member of Domain Users, Domain Admins, Administrators, and Backup Operators.

Add Backup Operators

Make the accounts of human users of Retrospect members of Backup Operators. Any login to be used with Retrospect on the backup computer must be a member of Backup Operators or Administrators.

Configure Retrospect Security Preference

After configuring the Retrospect backup user account, you must configure Retrospect to use the new account. Although you can configure Retrospect to run as a different domain user for each SQL server, or to use a given SQL login for each SQL server, it is easier and better to configure a particular preference so Retrospect runs as the Retrospect backup user for all SQL servers. The following steps describe how to set that preference. You can later configure different SQL server logins.

Log in to the backup computer using an administrator-privileged login.
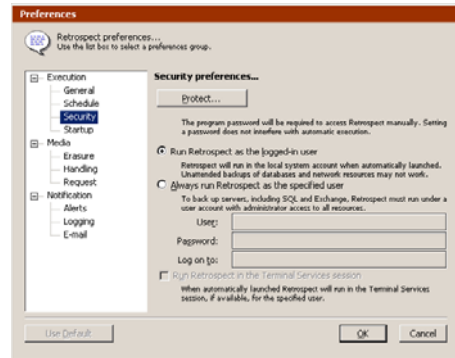
If you have not already done so, install Retrospect on the backup computer as described in Chapter 1 • Getting Started.

Launch the Retrospect application.

If this is the first time you have run Retrospect on the backup computer, the Getting Started Wizard displays. It includes a screen on which to enter user account information.

If this is not the first time you have run Retrospect on the backup computer, click Configure on the Retrospect navigation bar, then click Preferences. In the Execution preferences group, click Security.

Choosing the User Login

In both the preferences window and the first-launch user account window, the two radio buttons determine the user login under which the Retrospect application executes.

"Run Retrospect as the logged-in user" does so when you launch Retrospect manually (from the Start menu or Windows Explorer). When Retrospect automatically launches (to execute a script), it runs under the Local System account. Neither is ideal for use with SQL, because backups will likely fail due to lack of privileges. Therefore, do not select this preference.

"Always run Retrospect as the specified user" is the preferred setting for use with SQL. Click the radio button to select this preference. Enter the

Retrospect backup user name, password, and domain.

When you click OK to accept the security preference change, Retrospect may ask you to confirm your entry; click OK.

If Retrospect tells you the login is invalid, you may have mistyped the domain user name or password. Re-check the name and follow the above steps starting at "Create a Retrospect Backup User Account" on page 351.

When it verifies the specified domain user, Retrospect tells you to exit the application and re-launch for the change to take effect. Exit now and log off the administrator before taking the next step.

Verifying Proper Operation

Log in to the backup computer as a user who is a member of Backup Operators. Launch Retrospect and take note of its application window title, which includes the user the application is running as. Though you are logged in to the backup computer as a different user, the "user" running the application is the Retrospect backup user account.

Local Administrator Privileges

When you tell Retrospect to always run under a particular login, it assigns local administrator privileges to the login if it has none.

With the security preference set as described previously and a member of Backup Operators or Administrators logged in to the backup computer, Retrospect always runs with local administrator privileges, at minimum.

This means a backup operator could exploit administrator privileges in Retrospect to manipulate files on the local computer.

To provide additional security, consider using Retrospect's password protection preference to control user access to the Retrospect application.

INSTALLATION

If you have not already done so, install Retrospect on the backup computer as described in Chapter 1 • Getting Started. Set the security preference as described previously, under "Security" on page 350.

If you will use a SQL server as a Retrospect client, install the Retrospect client software on that computer. For details see Chapter 7 • Networked Clients.

Logging in the Client

If you are using a SQL server as a Retrospect client, log in the client from the backup computer. For details see Chapter 7 • Networked Clients.

Licensing and Logging In

Choose License Manager from the Window menu to see licensed components.

If SQL Database Backup is not listed, or if it is listed with no available licenses, click Add and enter a license code for SQL Database Backup. (Click Purchase to get a code from Roxio.)

After adding a SQL Backup license, it is listed as available for use. The next step is to use it.

Using a License

From the navigation bar, click Volumes to see the volumes database window. Under My Computer and Backup Clients are all the SQL servers known to Retrospect.
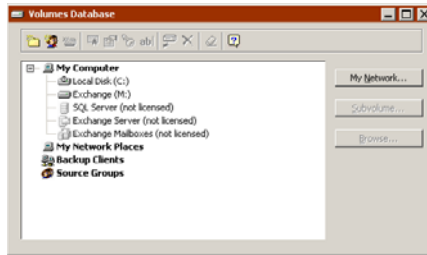
Their icons are grayed out because they are not yet licensed, as indicated by the text. Though there is a license available in the license manager, Retrospect does not know with which servers you want to use it. You must apply a license to each server you wish to use with Retrospect.

Click on the SQL server you want to work with, which makes Retrospect ask whether you wish to use an available license. Click OK. After a moment, the "not licensed" tag disappears from the SQL Server container.

If Retrospect does not do anything when you click SQL Server, or it asks you to enter a login for a local (non-client) server, the logged in user may not have sufficient privileges to access the SQL server or the service may not be running. Confirm the service is working and re-read "Security" on page 350 and set up security correctly before trying again.

SQL Server Login for a Client

For a server that is a client of Retrospect, Retrospect asks you to enter SQL server login information immediately after applying a license.

Follow the steps below.

Logging in to a SQL Server

For each SQL server, Retrospect lets you specify an authentication method other than the Retrospect backup user account.

For each SQL server that is a client of Retrospect, you must enter login information

for the SQL server immediately after applying its license.

For a just-licensed client, Retrospect already has the login window up. Otherwise, in the volumes database window, select a SQL server and click the Login as button on the toolbar.

Select an authentication method: Use SQL Authentication, Use Domain Authentication, or Use current RBU information (to authenticate using the Retrospect backup user account you supplied in the security preference). Enter the login information for your selected authentication method.

If Retrospect does not display the SQL server databases, or it tells you authentication failed, the specified user may not have sufficient privileges to access the SQL server on the client computer or the service may not be running. Confirm the service is working and re-read "Security" on page 350 and set up security correctly before trying again.

GENERAL USE

After licensing a SQL server, you can add it to your scripts, working with it in source and destination lists. You can also work with SQL servers in the volumes database window.

NOTE: You cannot archive SQL data.

Working with a Volumes List

From the navigation bar, click Configure> Volumes to display the Volumes Database window. Under My Computer and Backup Clients are all the SQL servers known to Retrospect.
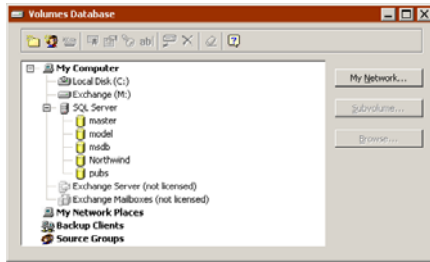
For each SQL server there is a SQL Server container under each computer operating as a SQL server. If you are running Retrospect on the server itself, the SQL container is under My Computer.
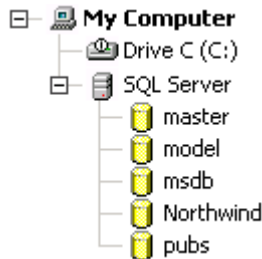
If you are not running Retrospect on the server, the SQL container is under Backup Clients.
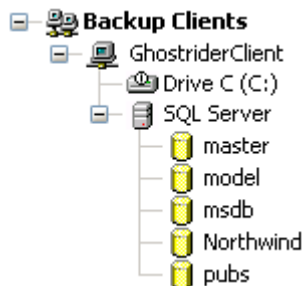
If a SQL Server container's icon is gray, or nothing is nested beneath it, Retrospect may be running as a user with insufficient privileges to see the SQL server data. If you use the SQL Server container in scripts they will fail when executed. Re-read "Security" on page 350 and set up security correctly.

If a SQL Server container's icon is colored and one or more items are nested beneath it, Retrospect is running as a user privileged to see the SQL server data. This means you set up the security correctly.

The SQL Server Container

Retrospect displays one SQL Server container per SQL server. It appears under My Computer when Retrospect is run locally on the server itself. For a SQL server that is a networked client of Retrospect, its SQL Server container appears under its computer's client container.

A SQL Server container includes one or more databases. Click the + or – controls of a SQL Server container to expose or hide its contents.

Selecting a SQL Server container as a backup source causes Retrospect to back up all of the server's databases.

If you do not wish to backup all databases within a given server, you can select one or more individual databases to be backed up. Individual databases appear under the SQL Server container.

Releasing a License

You can release Retrospect's license of a SQL server you no longer wish to back up or restore, making the license available for other use with other SQL servers.

Select a SQL container and click the Licensing button on the toolbar. Retrospect asks whether you wish to release the used license. Click OK to release it.

After releasing a SQL license, SQL containers and their databases become invalid in scripts.

BACKING UP

To back up a SQL server or a database, you can use a backup script or you can initiate an immediate backup. Each method uses the familiar

components of a backup: source, destination, selection criteria, and options.

For the source, select any one or combination of SQL Server containers and databases. Or, select My Computer or Backup Clients to back up a local SQL server or client SQL server, respectively.

For the destination, select any one or combination of Backup Sets.

Retrospect ignores selectors when backing up SQL databases. If your sources include both non-database volumes and SQL databases, Retrospect applies the specified selector to the non-database volumes only.

The SQL Server options group lets you determine the type of backup Retrospect should attempt for the source. Choose Full Backup, Differential Backup, Log Backup, or Log Backup No Truncate.

Retrospect cannot do any other type of backup unless the database has previously had a full backup. In this case it automatically attempts a full backup.

When implementing a scripted backup strategy, you will have separate scripts for the different backup types. For example, you might have a full backup script scheduled to run on Fridays and a differential backup script running daily.

For details on the available options, see "Windows SQL Server Options" on page 248.

Recovery Model

You must ensure a given database uses a recovery model (SQL 2000) or options (SQL 7) compatible with your desired types of backup. For example, Retrospect will report an error trying to do a log backup of a SQL database that uses the simple recovery model.

Backup Sets

Unlike backups of other data, database backups are not necessarily self-contained within a single Backup Set.

You are not assured you will be able to restore a database Snapshot from one set of media, as is the case with restoring files. Retrospect may require media from multiple Backup Sets to restore a given database, depending on your backup strategy and backup history.

DATABASE BACKUP HISTORY

Retrospect tracks each backup session of each database. You can view the history of these backups from Reports>Database Backup History.
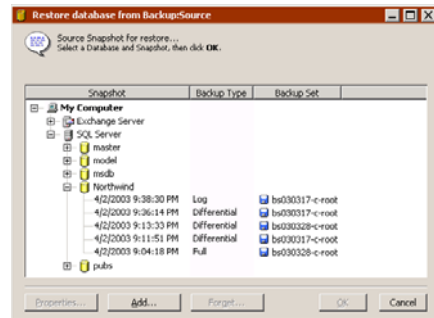
The window lists all of Retrospect's database session Snapshots of each SQL database. (Exchange databases and storage groups are also listed in this window.)

Using the buttons at the bottom of the window, you can view the properties of a Snapshot, add a database session from a Backup Set, or remove a Snapshot from this list.

Viewing the properties of a Snapshot shows you the Backup Set media required to restore the database.

RESTORING

To restore a SQL server or one or more databases, you can use a script or you can initiate an immediate restore. Each method uses the familiar components of a restore: source database Snapshot, destination server, chosen files (messages and folders from mailboxes only), and options.

Restoring a SQL Database

To restore a database from a SQL server backup, click Restore>Database (to initiate an immediate restore) or create a Restore Database script.
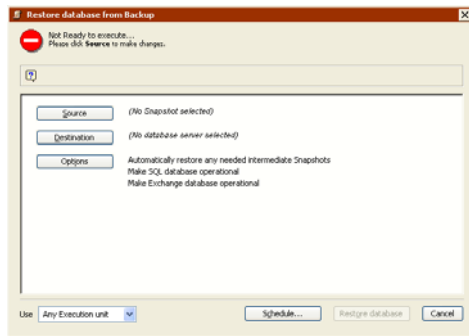
For the source, select a database Snapshot from which to restore.
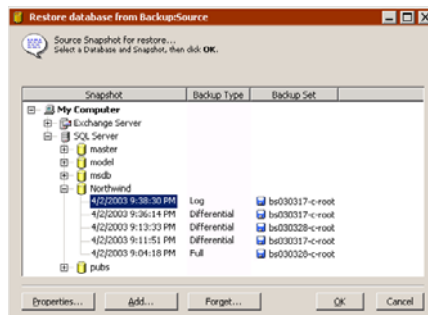
You can add and remove database Snapshots from this list with the Add and Forget buttons.

Set the destination for the database to be restored by selecting a SQL Server container.
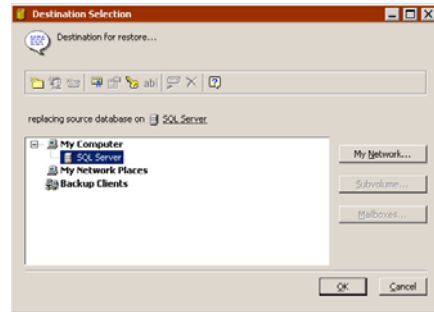
Click Options to specify execution options. For details on the available options, see "Windows SQL Server Options" on page 248 and "Restore Database Options" on page 240.
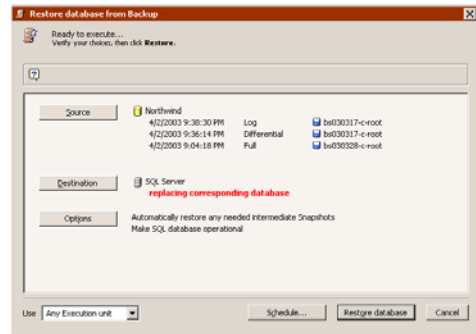
Notice how multiple sessions are listed below the source database Snapshot if its most recent backup was not the full backup type. This is because Retrospect has an execution option, on by default, that causes it to restore each session needed to completely restore the source.

Once your database restore operation is set up, you can save the script or proceed with the immediate restore.

DISASTER RECOVERY

After completely backing up a SQL server (system volume and databases), you can recover from a disastrous data loss.

First, follow the appropriate steps in "Restoring the Backup Computer" on page 207. Next, follow the steps below.

1. Restart Services

If you restored from a backup that used the Retrospect Open File Backup add-on to back up the SQL server (specifically, its master, model and msdb system databases), follow this step. If not, skip this step on continue with the next step.

These databases allow the SQL service to start after the SQL application has been restored. After all partitions on the system have been restored, verify the SQL services are running. If a service is not running, start it from SQL Server Service Manager or SQL Server Enterprise Manager.

If a SQL server lost its registration in Enterprise Manager, simply re-register it.

Skip the next step.

2. Rebuild then Restart Services

If you did *not* restore from a backup that used the Retrospect Open File Backup add-on to back up the SQL server (specifically, its master, model and msdb system databases), follow this step. If you did, skip this step and continue with the next step.

Use the Microsoft Search utility to find the rebuildm.exe utility on your system. Have your Microsoft SQL installation CD available.

Because the SQL service will not start without the master and other system databases, use the rebuildm.exe utility to rebuild the databases. Run the utility for each instance of SQL on the system. After the system databases are restored, verify the SQL service has started. Manually restart the service if needed.

3. Restore Databases in Single User Mode

Start the SQL server in single user mode from the SQL Server Enterprise Manager, not from the command line. Right-click on the server and choose Properties. Click Setup Parameters and

add new parameter -m. Stop and restart the SQL service using SQL Server Service Manager. The SQL server is now running in single user mode and all services are running with the same user ID.

Use Retrospect to restore only the master database from its most recent database Snapshot.

After completing the restore operation, remove the -m option, then stop and restart the SQL server to return to normal mode.

4. Delete Suspect Databases

After completing the previous step, there are databases in the SQL Enterprise Manager that are grayed out and marked as suspect. This is because the master database contains a record of all the databases for that server and any databases which lack an associated data file are suspect. Delete all suspect databases on SQL 7 servers to ensure the next step is successful.

5. Restore Databases

Use Retrospect to restore the msdb database, then restore all other databases, always restoring from the most recent database Snapshot. After you have restored all SQL databases for each SQL server, your system is ready for use.

TIP: See the SQL Enterprise Manager logs for details on errors reported by Retrospect.

EXCHANGE SERVER AGENT

- **REQUIREMENTS**

- **SECURITY**

- **INSTALLATION**

- **GENERAL USE**

- **BACKING UP**

- **DATABASE BACKUP HISTORY**

- **RESTORING**

- **DISASTER RECOVERY**

The Retrospect Exchange Server Agent provides the ability to back up and restore Microsoft Exchange servers. Without the agent add-on, Retrospect cannot back up the databases and mailboxes of Exchange stores.

You can back up an Exchange server locally, running the Retrospect application on the server itself, or you can back up the Exchange server as a Retrospect client, running the Retrospect application on a different computer.

REQUIREMENTS

There are different minimum requirements of Retrospect, Exchange, and Windows, as described below.

Exchange Server

The Retrospect Exchange Server Agent works with the following combinations of operating system software and database software.

- Exchange 2003, Windows Server 2003
- Exchange 2000, Windows 2000 Server
- Exchange 5.5, Windows 2000 Server
- Exchange 5.5, Windows NT 4.0 Server

Exchange Server Running Retrospect Application

To use an Exchange server as the backup computer, running the Retrospect application on the server itself, one of the following application licenses is required:

- Retrospect Disk-to-Disk
- Retrospect Single Server
- Retrospect Small Business Server
- Retrospect Multi Server

You can upgrade the Retrospect application to a more powerful edition by entering a license code purchased from Roxio.

Exchange Server as Retrospect Client

To back up an Exchange server as a client, the backup computer must run Retrospect Multi Server (or Retrospect Disk-to-Disk, Small Business Server, or Single Server, with a server client) under one of the following operating systems:

- Windows NT 4.0
- Windows 2000
- Windows XP
- Windows Server 2003

SECURITY

Numerous security measures prevent an unauthorized user from simply launching Retrospect on the backup computer and backing up an Exchange server. Because Exchange can only be backed up and restored by a domain administrator, you must prepare Retrospect to run in the correct security context. This involves configuring preferences in Retrospect so that the application or Retrospect client software runs as a certain user with sufficient privileges for the Exchange server.

Regardless of whether you have yet installed or run Retrospect, and regardless of how you previously set its security preference, follow these instructions to ensure you can work with Exchange.

Create and Manage User Logins

You must create a special login for use by Retrospect and identify human users of Retrospect as Backup Operators. These steps, which use Active Directory Users and Computers (Windows 2000) or User Manager for Domains and (Windows NT 4.0), are described below.

Create a Retrospect Backup User Account

Within the Exchange server's domain, create a login dedicated for use by Retrospect, such as RBU (for Retrospect backup user account).

Make this account a member of Domain Users, Administrators, Backup Operators, and Domain Admins. Also give it an Exchange mailbox. In Exchange 5.5, you must use User Manager for Domains and Microsoft Exchange Administrator for some of these tasks.

Send an e-mail message to this Retrospect backup account to initialize it in Exchange.

Add Backup Operators

Make the accounts of human users of Retrospect members of Backup Operators. Any

login to be used with Retrospect on the backup computer must be a Backup Operator or Administrator.

Configure Retrospect Security Preference

After configuring the Retrospect backup user account, you must configure Retrospect to use the new account. Although you could configure Retrospect to run as a different domain user for each Exchange server, it is easier and better to configure a particular preference so Retrospect runs as the Retrospect backup user for all Exchange servers.

Log in to the backup computer using an administrator-privileged login.

If you have not already done so, install Retrospect on the backup computer as described in Chapter 1 • Getting Started.

Launch the Retrospect application.

If this is the first time you have run Retrospect on the backup computer, the Getting Started Wizard displays. It includes a screen on which to enter user account information.

If this is not the first time you have run Retrospect on the backup computer, click Configure on the Retrospect navigation bar, then click Preferences. In the Execution preferences group, click Security.

Choosing the User Login

In both the preferences window and the first-launch user account window, the two radio buttons determine the user login under which the Retrospect application executes.

"Run Retrospect as the logged-in user" does so when you launch Retrospect manually (from the Start menu or Windows Explorer). When Retrospect automatically launches (to execute a script), it runs under the Local System account. Neither is ideal for use with Exchange, because backups will likely fail due to lack of privileges. Therefore, do not select this preference.

"Always run Retrospect as the specified user" is the preferred setting for use with Exchange. Click the radio button to select this preference. Enter the Retrospect backup user name, password, and domain.

When you click OK to accept the security preference change, Retrospect may ask you to confirm your entry; click OK.

If Retrospect tells you the login is invalid, you may have mistyped the domain user name or password. Re-check the name and follow the above steps starting at "Create a Retrospect Backup User Account" on page 360.

When it verifies the specified domain user, Retrospect tells you to exit the application and re-launch for the change to take effect. Exit now

and log off the administrator before taking the next step.

Verifying Proper Operation

Log in to the backup computer as a user who is a member of Backup Operators. Launch Retrospect and take note of its application window title, which includes the user the application is running as. Though you are logged in to the backup computer as a different user, the "user" running the application is the Retrospect backup user account.

Local Administrator Privileges

When you tell Retrospect to always run under a particular login, it assigns local administrator privileges to the login if it has none.

With the security preference set as described previously and a member of Backup Operators or Administrators logged in to the backup computer, Retrospect always runs with local administrator privileges, at minimum.

This means a backup operator could exploit administrator privileges in Retrospect to manipulate files on the local computer.

To provide additional security, consider using Retrospect's password protection preference to control user access to the Retrospect application.

INSTALLATION

If you have not already done so, install Retrospect on the backup computer as described in Chapter 1 • Getting Started. Set the security preference as described previously, under "Security" on page 360.

If you will use an Exchange server as a Retrospect client, install the Retrospect client software on that computer. For details see Chapter 7 • Networked Clients.

Logging in the Client

If you are using an Exchange server as a Retrospect client, log in the client from the backup computer. For details see Chapter 7 • Networked Clients.

Licensing

Choose License Manager from the Window menu to see licensed components.

If Exchange Database/Mailbox Backup is not listed, or if it is listed with no available licenses, click Add and enter a license code for Exchange Database/Mailbox Backup. (Click Purchase to get a code from Roxio.)

After adding an Exchange Backup license, it is listed as available for use. The next step is to use it.

Using a License

From the navigation bar, click Volumes to see the volumes database window. Under My Computer and Backup Clients are all the Exchange servers known to Retrospect.
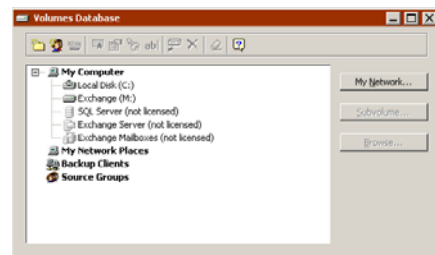
Their icons are grayed out because they are not yet licensed, as indicated by the text. Though there is a license available in the license manager, Retrospect does not know with which servers you want to use it. You must apply a license to each server you wish to use with Retrospect.

Click on the Exchange server you want to work with, which makes Retrospect ask whether you wish to use an available license. Click OK. After a moment, the "not licensed" tags disappear from the Exchange Server container and its attendant Exchange Mailboxes container.

If Retrospect does not do anything when you click Exchange Server, the logged in user may not have sufficient privileges to access the Exchange server or the service may not be running. Confirm the service is working and re-read "Security" on page 360 and set up security correctly before trying again.

Exchange Container Properties for a Client

For a server that is a client of Retrospect, Retrospect will let you enter Exchange server authentication information immediately after applying a license.

Have Retrospect use the Retrospect backup user account you supplied in the security preference.

If Retrospect does not display the Exchange server contents, or it tells you authentication failed, the specified user may not have sufficient privileges to access the Exchange server on the client computer or the service may not be running. Confirm the service is working and re-read "Security" on page 360 and set up security correctly before trying again.

GENERAL USE

After licensing an Exchange server as described previously, you can add it to your scripts, working with it in source and destination lists. You can also work with Exchange servers in the volumes database window.

NOTE: You cannot archive Exchange data.

Working with a Volumes List

From the navigation bar, click Configure> Volumes to display the Volumes Database window. Under My Computer and Backup Clients are all the Exchange servers known to Retrospect.
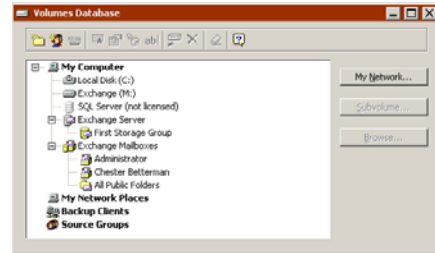
For each Exchange server there is an Exchange Server container and its attendant Exchange Mailboxes container. There is one pair of containers organized under each computer operating as an Exchange server. If you are running Retrospect on the server itself, the Exchange containers are under My Computer.

If you are not running Retrospect on the server, the Exchange containers are under Backup Clients.
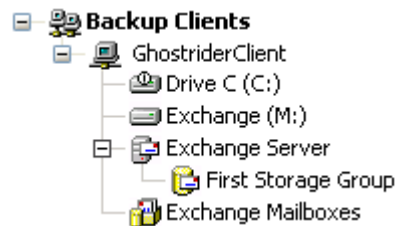
If an Exchange Server container's icon is gray, or nothing is nested beneath it, Retrospect may be running as a user with insufficient privileges

to see the Exchange server data. You can use the Exchange Server container in scripts but they will fail when executed, and you cannot use Exchange Mailboxes. Re-read "Security" on page 360 and set up security correctly.

If an Exchange Server container's icon is colored and one or more items are nested beneath it, Retrospect is running as a user privileged to see the Exchange server data. This means you set up the security correctly.

About the Exchange Virtual Drive

As part of its default installation, Exchange 2000 creates a virtual drive and maps it to the drive letter M. *This data on this drive is not useful for backing up and restoring.*

WARNING: Backing up the Exchange M: drive will not back up your Exchange Server and its data. Restoring to the Exchange M: drive will not restore your Exchange Server and its data.

In Retrospect, the Exchange M: drive appears under the computer container (My Computer or a client computer), but Retrospect does not include the Exchange M: drive when you use its parent container in an operation. For example, selecting a client container as a backup source causes its C: drive hard disk to be backed up, but not its M: virtual drive.

Retrospect ignores the Exchange M: drive because it contains no data you can back up and restore.

Instead use the Exchange Server and Exchange Mailboxes containers as instructed under "Backing Up" on page 366 and "Restoring" on page 367.

The Exchange Server Container

Retrospect has one Exchange Server container per Exchange server. It is under My Computer when Retrospect is run locally on the server itself. For an Exchange server that is a networked

client of Retrospect, its Exchange Server container appears under its computer's client container.

An Exchange Server container includes one or more storage groups or databases. Click the + or – controls of an Exchange Server container to expose or hide its contents.

Selecting an Exchange Server container as a backup source causes Retrospect to back up all of the server's databases or storage groups.

If you do not wish to back up all stores within a given server, you can select one or more individual databases or storage groups to be backed up.

Individual Storage Groups

Individual databases (Exchange 5.5) and storage groups (Exchange 2003, Exchange 2000) appear under the Exchange Server container.

Each storage group includes one or more public folder stores and one or more mailbox stores. These stores are not otherwise visible in Retrospect but you can browse a storage group and see its stores represented as database files.

Selecting an individual storage group as a backup source causes Retrospect to back up all of the group's public folder stores and mailbox stores. You cannot isolate specific stores to be backed up.

The Exchange Mailboxes Container

Retrospect has one Exchange Mailboxes container per Exchange server. It is under My Computer when Retrospect is run locally on the server itself. For an Exchange server that is a networked client of Retrospect, its Exchange Mailboxes container appears under its client computer container.

An Exchange Mailboxes container can include:

• one or more individual mailboxes

• the All Public Folders container

When you license an Exchange Server, Retrospect automatically adds all the mailboxes associated with that server to the Exchange Mailboxes container. If, at a later time, you create new mailboxes or delete mailboxes, Retrospect modifies the contents of the Exchange Mailboxes container.

The All Public Folders container is also automatically added to the Exchange Mailboxes container.

NOTE: The Exchange Mailboxes container can include mailboxes from multiple mailbox stores and Public Folders from multiple public folder stores.

Selecting the Exchange Mailboxes container as a backup source causes Retrospect to back up all mailboxes. This allows you to restore an individual mailbox, mailbox folder, or even a single message.

WARNING: Backing up the Exchange Mailboxes container is not a substitute for backing up the entire Exchange server.

In order to back up Public Folders, you must select either All Public Folders, or the individual Public Folders you want to back up. Selecting the All Public Folders container allows you to restore an individual Public Folder or even a single message in a Public Folder.

WARNING: If you select just the Exchange Mailboxes container, Retrospect does not back up any Public Folders.

Individual Mailbox Folders and Public Folders

Before you can back up an individual mailbox folder or Public Folder, you must add it to the Volumes Database.

To add a Mailbox Folder:

1. Choose Configure>Volumes from the Retrospect navigation bar.

2. In the Exchange mailboxes container, select a mailbox, then click the Subvolume button.
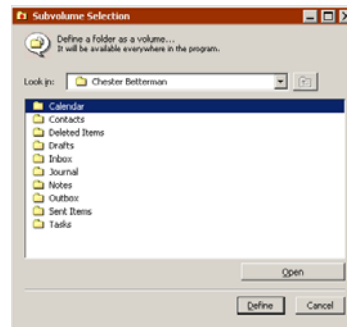
Retrospect displays a list of all the folders available for that mailbox.

3. Select one or more folders from the list and click Define.

Retrospect adds the folders to the Volumes Database.

To add a Public Folder:

1. Choose Configure>Volumes from the Retrospect navigation bar.

2. In the Exchange mailboxes container, select All Public Folders, then click the Subvolume button.

Retrospect displays a list of all available Public Folders.

3. Choose one or more Public Folders from the list and click Define.

Retrospect adds the Public Folders to the Volumes Database.

Once you have added mailbox folders and/or Public Folders, they appear in the Volumes Database. Click the + or −controls of an Exchange Mailboxes container to expose or hide its contents.
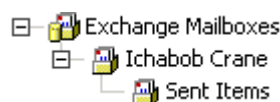
Defining an individual mailbox folder or Public Folder allows Retrospect to back it up as a unique entity instead of as a part of a larger container.

To back up an individual mailbox folder or Public Folder, select it under the Exchange Mailboxes container.

Releasing a License

You can release Retrospect's license of an Exchange server you no longer wish to back up or restore, making the license available for other use with other Exchange servers.

Select an Exchange container and click the Licensing button on the toolbar. Retrospect asks whether you wish to release the used license. Click OK to release it.

After releasing an Exchange license, Exchange containers, storage groups, and mailboxes become invalid in scripts.

BACKING UP

To back up an Exchange server, a storage group, a mailbox, or a Public Folder, you can use a backup script or you can initiate an immediate backup. Each method uses the familiar components of a backup: source, destination, selection criteria, and options.

NOTE: Exchange 2003 includes a Recovery Storage Group feature that allows you to mount a second copy of an Exchange mailbox store on the same server as the original database. Retrospect does not support backing up recovery storage groups.

For the source, select any one or combination of Exchange Server container, storage group, Exchange Mailboxes container, individual mailbox, individual mailbox folder, individual Public Folder, or the All Public Folders container.

Or, select My Computer or Backup Clients to back up a local Exchange server or client Exchange server, respectively. If you select My Computer or Backup Clients, Retrospect backs up everything in the container, including all mailboxes and All Public Folders.

TIP: If your sources include Exchange mailboxes or Public Folders, as well as non-Exchange volumes, make sure to group mailboxes and Public Folders together. This results in faster performance when backing up to tape Backup Sets with verification on.

For the destination, select any one or combination of Backup Sets.

Retrospect ignores selectors when backing up Exchange databases. If your sources include both non-database volumes and Exchange databases, Retrospect applies the specified selector to the non-database volumes only.

When backing up Exchange mailboxes, Retrospect *does* apply selectors. Retrospect includes two conditions that are especially useful for creating custom selectors to apply to Exchange mailbox backups; the Sender condition (from the Mailbox group) and the Date condition (from the Universal group). For more information, see "Using Selectors" on page 291.

When backing up an individual mailbox, you can set the file selection criteria to back up messages based on mailbox sender and universal date conditions. In a scripted backup, create a custom selector. In an immediate backup, mark items to back up in the preview browser. You can use its Find command to search for messages. Choosing up a subset of messages helps lessen the performance degradation associated with backing up mailbox messages.

The Exchange Server options group lets you determine the type of backup Retrospect should attempt for the source. Choose Full Backup,

Differential Backup, or Log/Incremental Backup.

Retrospect cannot do a differential backup or log/incremental backup of data unless it has previously had a full backup. In this case it automatically attempts a full backup.

When implementing a scripted backup strategy, you will have separate scripts for the different backup types. For example, you might have a full backup script scheduled to run on Fridays and a differential backup script running daily.

For details on the available options, see "Windows Exchange Server Options" on page 249.

Circular Logging

You must ensure a given Exchange server does not use circular logging if you wish to do differential or log backups. For example, Retrospect will report an error trying to do a differential backup of a Exchange server that uses circular logging.

Circular logging is enabled by default in Exchange 5.5 and disabled by default in Exchange 2003 and Exchange 2000.

Backup Sets

Unlike backups of other data, database backups are not necessarily self-contained within a single Backup Set.

You are not assured you will be able to restore a database Snapshot from one set of media, as is the case with restoring files. Retrospect may require media from multiple Backup Sets to restore a given database, depending on your backup strategy and backup history.

DATABASE BACKUP HISTORY

Retrospect tracks each backup session of each database or storage group. You can view the history of these backups from Reports> Database Backup History.
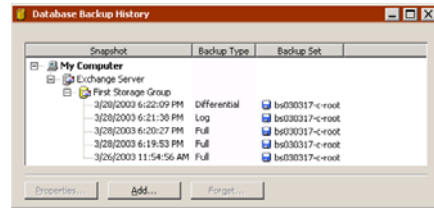
The window lists all of Retrospect's database session Snapshots of each Exchange database or storage group. (SQL databases are also listed in this window.)

Using the buttons at the bottom of the window, you can view the properties of a Snapshot, add a database session from a Backup Set, or remove a Snapshot from this list.

Viewing the properties of a Snapshot shows you the Backup Set media required to restore the database.

RESTORING

To restore an Exchange server, a storage group, a mailbox, or one or more messages, you can use a script or you can initiate an immediate restore. Each method uses the familiar components of a restore: source database or mailbox Snapshot, destination server or mailbox, chosen files (messages and folders from mailboxes only), and options.

NOTE: Exchange 2003 includes a Recovery Storage Group feature that allows you to mount a second copy of an Exchange mailbox store on the same server as the original database. Retrospect does not support restoring to recovery storage groups. In addition, to restore data to an Exchange 2003 server that includes a recovery storage group, you must either delete the recovery storage group before restoring, or create a Recovery SG Override registry key on the Exchange server as described on Microsoft's web site.

Restoring an Exchange Storage Group or Database

To restore a storage group or database from an Exchange server backup, click Restore> Selected Database (to initiate an immediate restore) or create a Restore Database script.
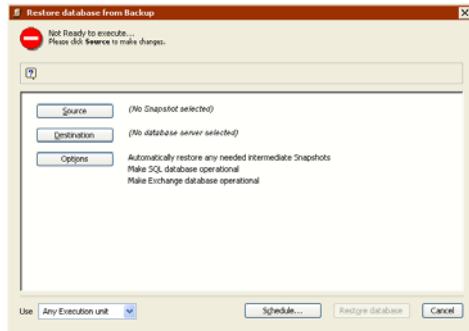
For the source, select a database Snapshot.
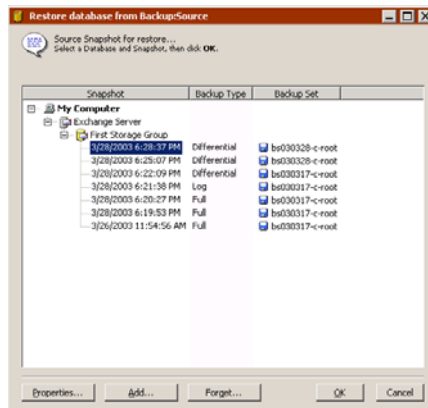
You can add and remove database Snapshots from this list with the Add and Forget buttons.

Set the destination for the database to be restored by selecting an Exchange Server container.
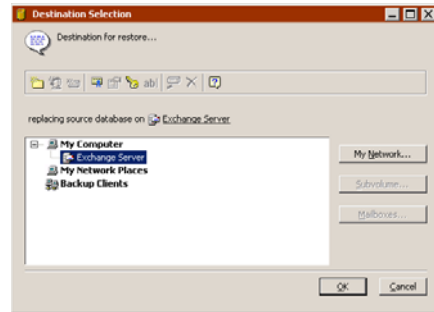
Click Options to specify execution options. For details on the available options, see "Windows Exchange Server Options" on page 249 and "Restore Database Options" on page 240.
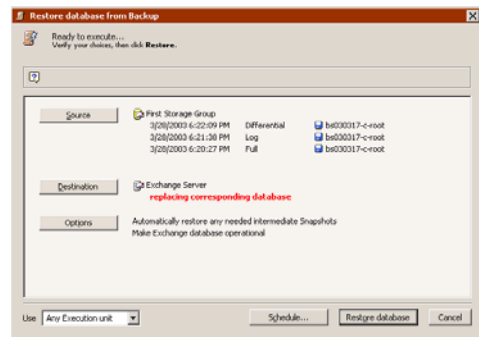
Notice how multiple sessions are listed below the source database Snapshot if its most recent backup was not the full backup type. This is because Retrospect has an execution option that causes it to restore each session needed to completely restore the source.

Once your database restore operation is set up, you can click Schedule to save the settings as a script, or proceed with the immediate restore.

Restoring a Mailbox or Public Folder

To restore an individual mailbox, an individual Public Folder, all Public Folders, or one or more specific messages, click Restore>Mailbox from the navigation bar.
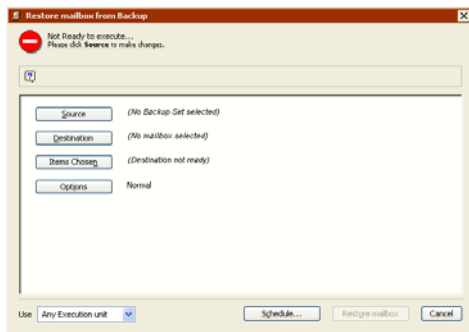
For the source, select a Snapshot for a mailbox, Public Folder, or All Public Folders.
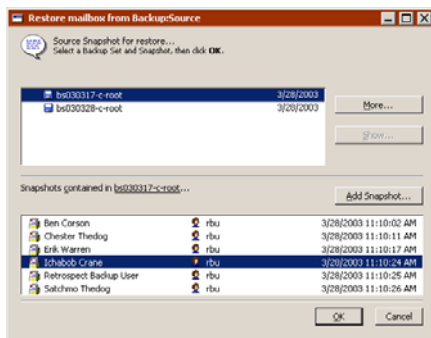
Set the destination by selecting an individual mailbox, an individual Public Folder, or the All Public Folders container. Set the list box to Retrieve Messages & Folders or Retrieve Just Messages.
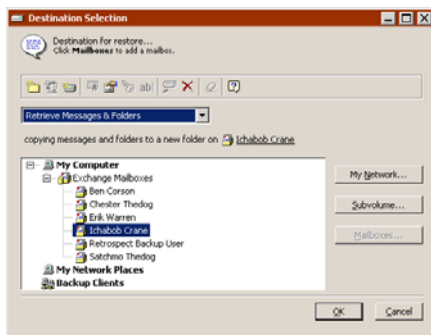
In an immediate restore, choose items to restore in the browser. You can use the Find command to search for messages based on mailbox sender and universal date conditions.

In a scripted restore, you can only restore an entire mailbox or Public Folder.

Click Options to specify execution options.
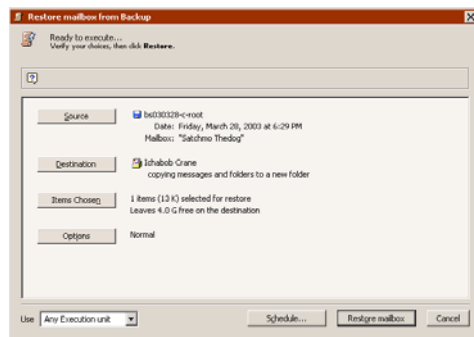
Once your restore operation is set up, you can save the script or proceed with the immediate restore.

DISASTER RECOVERY

After completely backing up an Exchange server (system volume and databases), you can recover from a disastrous data loss.

First, follow the appropriate steps under "Restoring the Backup Computer" on page 207.

Next, follow the steps below for your version of Microsoft Exchange.

TIP: The Roxio Retrospect Knowledgebase (www.retrospect.com/knowledgebase) includes more detailed articles on Exchange disaster recovery.

Exchange 2003 and Exchange 2000

After restoring the rest of the computer, restart the Exchange services but make sure the databases are not mounted. Delete everything from the storage group folder or folders. This ensures the log files match the databases and allows you

to remount the stores after restoring the databases.

After everything is deleted, restore the databases. (For more information, see "Restoring an Exchange Storage Group or Database" on page 368.)

After restoring, the databases should be mounted and ready for use.

Exchange 5.5

After restoring the rest of the computer, make sure the Exchange services are stopped. Delete everything from the mdbdata and dsadata folders (default installation names). This ensures the log files match the databases and allows you to restart the services after restoring the databases.

After everything is deleted, restore the databases. (For more information, see "Restoring an Exchange Storage Group or Database" on page 368.)

After restoring, the services should be started and ready for use.

GLOSSARY

access privileges – The privileges given to (or withheld from) users to see folders, see files, and make changes to shared volumes.

append – To write additional data to a Backup Set. In a Normal backup, Retrospect appends file data to the current Backup Set member.

archive (verb) – To copy files from a volume to a Backup Set. For example, "Let's archive these QuickTime movies." Archiving may, optionally, involve removing the copied files from the source. Also see **back up**.

archive (noun) – 1. An operation in which files are archived. For example, "The archive was successful last night." 2. An entity of backup materials. For example, "Retrieve the 1997 accounts from the archive." In this respect, a Backup Set is an archive. Also see **Backup Set**.

ASPI (Advanced SCSI Programming Interface) – Software which manages communication among peripheral devices. This combination of integrated software is known as the ASPI layer.

ATAPI (ATA Packet Interface) – A standard for connecting peripheral devices such as CD-R drives and tape drives to a computer's IDE interface. ATAPI allows you to easily attach additional devices to your computer.

back up (verb) – To copy files from a volume to a Backup Set (such as CD-R or CD-RW, cartridges, or floppy disks). You should back up regularly in case something happens to your hard disk or any files.

backup (noun) – 1. An operation in which files are backed up. For example, "I just did today's backup." 2. An entity of backup materials. For example, "Fortunately, we can get the backup from the safe and restore the files." In this respect, a Backup Set is a backup. Also see **back up** and **Backup Set**.

backup action – See **Recycle backup, New Backup Set backup, New Member backup,** and **Normal backup.**

Backup Clients – The Backup Clients container holds client computers which are logged in to Retrospect.

backup computer – The computer on which you are using Retrospect with a backup device. In a networked environment, it is the computer used to back up client computers.

backup date – The most recent date and time a Mac OS file, folder, or volume was copied to a Backup Set. Retrospect sets this date for volumes, folders, and/or files *only* when you check the appropriate boxes in the Macintosh client options. Also see **creation date** and **modification date**.

Backup Report – Displays all known volumes with information about when they were last backed up.

Backup Set – A set of storage media and Catalog. Retrospect stores all files in Backup Sets. There are different types of Backup Sets for different media and devices: disk Backup Sets for removable and fixed disks, file Backup Sets for a single volume, tape Backup Sets for tape cartridges, and CD/DVD Backup Sets for recordable and rewriteable compact disc drives.

browser – Retrospect's tool that allows you to view the folder and file structure of a volume or contents of a Backup Set. You can also use a browser to see the files and folders in a Backup Set. The browser allows you to manipulate files and mark them to be worked within an operation such as a backup.

Catalog – Retrospect's index of the files and folders contained in a Backup Set. The Catalog File allows you to mark files for restore or retrieval without having to load or insert your Backup Set media.

CD/DVD Backup Set – For use with recordable compact discs (CD-R, CD-RW, DVD-R, DVD-R DL, DVD-RW, DVD+R, DVD+R DL, or DVD+RW). Also see **Backup Set**.

client – A networked Windows, UNIX, NetWare, or Macintosh computer with Retrospect client software whose volumes are available for backup by the backup computer. Also see **backup computer**.

compression – Reduces the size of the data being copied to the Backup Set media in a backup or archive. Retrospect can do it with software compression, or a capable tape drive can do it with hardware compression.

condition – In Retrospect's file selectors, a distinguishing criterion relating to file or folder characteristics. You can choose multiple condi-

tions to make your own custom selectors. Also see **selector**.

Config75.dat file – The file containing your custom settings, including known Backup Sets, scripts, security codes, preferences, custom selectors, and client login names. This file is automatically created the first time you start Retrospect, and is used while Retrospect is open. If you delete this file, all of your custom information will be lost and the default configurations will be used.

configured subnet – A **subnet** that Retrospect has been configured to search for clients.

container – An item for organizing other items such as volumes or clients in certain Retrospect windows. Also see **My Computer, My Network Places,** and **Backup Clients**.

Contents Report – A Retrospect report that shows a single Backup Set in terms of the sessions it contains. A list of all sessions is displayed for each Backup Set. Double-clicking a session creates a browser of all files in that session.

creation date – The time and date a file, folder or volume was created. A file's creation date is set when the file is first saved or made. A folder's creation date is set when you select make a new folder. A volume's creation date is set any time the volume is formatted or erased. With Windows file systems, a copied item's creation date changes to the date of the copy. Also see **backup date** and **modification date**.

creator code – The four-letter code that represents the creator of a file with the Macintosh HFS file system. For example, documents created by SimpleText have a creator code of ttxt. Retrospect lets you select files according to creator code.

day of week scheduler – A type of scheduler that lets you schedule a script to run every week

on specified days of the week (for example, every Monday, Wednesday, and Friday).

destination – The storage medium to which files are being moved, copied, or otherwise transferred. When backing up or archiving, the destination is a Backup Set. When restoring or duplicating, the destination is a volume.

device – Any piece of peripheral equipment connected to your computer, such as a hard disk drive, removable disk drive, or CD-RW drive. In this manual, the term "backup device" refers to any device that accepts Backup Set media, such as a CD-R drive or tape drive.

directory – A hierarchical structure on a volume that may contain files or more directories. These are known as **folders** in the desktop metaphor used by Windows and the Mac OS.

Disaster Recovery – The process used to restore a computer that has ceased to function. This involves installing a temporary OS and then restoring the entire hard disk from a Retrospect backup.

disc – A CD-R, CD-RW, DVD-R, DVD-R DL, DVD-RW, DVD+R, DVD+R DL, or DVD+RW medium. Compare to **disk**.

disk – Retrospect uses the term disk to refer to fixed disks, network volumes, or removable disks (e.g., Zip, DVD-RAM, MO). This manual uses the term disk in two contexts: 1. as a Windows Explorer-accessible volume for general storage; and 2. as a medium for use in a disk Backup Set. Compare to **disc**.

disk Backup Set – For use with fixed disks, network volumes, or removable disks. Also see **Backup Set**.

encryption – A way of encoding data so that it cannot be used by others without the password.

Exchange Agent – Retrospect's Exchange Agent provides specialized support for optimal-

ly backing up Microsoft Exchange 5.5, 2000, and 2003 servers.

file Backup Set – This type of Backup Set combines the Catalog and the data in a single file. The Backup Set media must be a single volume that is accessible from Windows Explorer, such as a file server or hard disk. Also see **Backup Set**.

file header information – A file's name, size, dates, and other attributes. This information is part of every file, and is also indexed in a Backup Set's Catalog.

file server – A computer running file server software, which allows users to share information over a network.

FireWire – Apple Computer's proprietary name for **IEEE 1394**.

folder – 1. A **directory** on a volume. 2. A Retrospect container for organizing items such as scripts, volumes, or clients.

Forget – The Forget toolbar icon allows you to remove an item from certain windows. Use Forget to clear listings for volumes, Subvolumes, clients, or Backup Sets you no longer wish to use. Note that "forgetting" a backup source volume does not affect any of the Backup Sets it has been backed up to; its files may be restored at any time as long as the Backup Set media is intact.

grooming – An option for disk Backup Sets. If you set a grooming policy for a disk Backup Set, Retrospect automatically deletes older files and folders from the disk when it runs out of disk space, in order to save newer files and folders.

group – A Retrospect container for organizing items such as volumes and clients.

IEEE 1394 – A specification of mechanical, electrical, and functional standards which lets a

computer connect and communicate with storage devices, such as hard disks and removable cartridge drives, and other peripheral devices, such as scanners and video camcorders. IEEE 1394 allows you to easily attach additional devices to your computer. IEEE 1394 technology is also known as 1394, i.LINK, or **FireWire**.

local subnet – The **subnet** in which the backup computer resides.

marking – Selecting files in the browser to be backed up or restored. Files can be marked (or unmarked) manually, or they can be marked according to various criteria using file selectors. In the browser, a check mark appears next to any marked file. Files that are highlighted in the browser are not necessarily marked.

matching – The scheme for comparing file attributes to determine whether files are identical, which then allows intelligent copying to avoid redundancy. Also see **Progressive Backup**.

medium – Any hard drive, disc, tape, floppy disk, or cartridge to which files can be copied. In this manual, media usually refers to the removable media of a Backup Set.

member – An individual **medium** (such as a floppy disk, CD, tape, or cartridge) used in a Backup Set.

modification date – The time and date a file was last changed. This date is automatically attached to the file by the computer's file system. A file's modification date is reset any time you make changes and save the file (see "backup date" and "creation date"). A folder's modification date is updated any time a folder or file is added, changed or removed from it.

My Computer – Retrospect's container that holds local volumes available from the backup computer.

My Network Places – Retrospect's container that holds network volumes available from the backup computer.

New Backup Set backup – Allows you to periodically introduce new media into your backups, keeping the original BackupSet media and Catalog intact for archival purposes. A New Backup Set backup copies all selected files to a new Backup Set of the same name as the old, with the addition of a generation number, such as "Backup Set A [001]."

Normal backup – Retrospect's usual backup action, performing an incremental backup to copy new or changed files.

Open File Backup – Retrospect's Open File Backup allows files to be backed up even if they are opened and being used. This is important to ensure proper backup of server applications such as customer relationship management applications and accounting packages, which are up and running 24 hours a day. For desktop and notebook computers, files such as those that contain e-mail messages or calendar appointments can be backed up while they are in use.

Operations Log – A Retrospect report that tracks all actions by Retrospect. The Operations Log documents all start-ups, executions, errors, and completions, as well as information on the number of files copied, duration of backup, and backup performance.

Piton – Retrospect's own proprietary protocol for communicating with backup **clients**. In the live network window, Retrospect uses the Piton name service to establish contact with clients.

Proactive Backup – Retrospect's technology allowing flexible, resource-driven or user-initiated backups.

Progressive Backup – A backup that intelligently copies only files that are new or have changed since the previous backup. Retrospect

usually backs up progressively with its Normal backup action. See also **matching**.

Recycle backup – A Recycle backup is useful to periodically reset a Backup Set so that it does not grow out of control. A Recyclebackup completely erases the Backup Set and Catalog before copying all selected files to the Backup Set. All previous data in the Backup Set is lost.

repeating interval scheduler – A type of scheduler that lets you schedule a script to repeat automatically at a specified interval of time, such as once every three weeks.

restore – An operation which copies files from a Backup Set to a volume.

root – The highest level of folders in a data structure. When you select a drive icon from the Windows Explorer, you see the root folders and files.

run document – A file that automatically starts a Retrospect script when opened. A run document allows you to run predefined Retrospect scripts by double-clicking on the run document file.

scheduler – A script element that lets you schedule a script to automatically execute at dates and times of your choice. Also see **day of week scheduler**, **repeating interval scheduler**, and **single date scheduler**.

script – A saved backup procedure that you can schedule to run at some future date and time or on a repeating schedule, such as daily. You can create as many scripts as you want.

SCSI (Small Computer System Interface) – A specification of mechanical, electrical, and functional standards for connecting peripheral devices such as hard drives or tape drives. SCSI allows you to easily attach additional devices to your computer.

SCSI terminator – A device used on a SCSI chain to maintain the integrity of signals on the chain.

selector – A feature that lets you search for or filter files which match certain conditions. You can use Retrospect's standard selectors, or create your own custom selectors. Also see **browser**.

session – A group of files from a single operation stored within a Backup Set.

single date scheduler – A type of scheduler that lets you schedule a script to automatically run at a specific date and time.

SMART (Self-Monitoring Analysis and Reporting Technology) – A technology built in to some hard disk drives that monitors and analyzes a drive's mechanical attributes over time and attempts to predict and report pending drive failure.

Snapshot – A Retrospect Snapshot is created during a backup operation to depict a volume's state (that is, all its files and the folder paths to them). It makes it easy to restore a hard disk to its exact state as of a given backup.

source – In a backup, duplicate, or archive operation, the volume from which files are copied. In a restore, the Backup Set from which files are copied.

staged backup – A backup strategy that involves backing up to disk, then transferring the backups to tape. This takes advantage of the benefits of both disk and tape.

subnet – A group of local computers physically networked together without a router or gateway, though they may use a gateway to connect to other networks. Also see **configured subnet** and **local subnet**.

Subvolume – A folder you designate as an independent volume for use within Retrospect.

tape Backup Set – For use with tape drives. Also see **Backup Set**.

TCP/IP – An industry standard network protocol. It is the standard protocol of the Internet, web servers, and FTP servers. It is the protocol used by Retrospect clients.

USB (Universal Serial Bus) – A specification of mechanical, electrical, and functional standards for connecting peripheral devices (keyboards, removable cartridge drives, printers) to the USB-capable computers. USB allows you to easily attach additional devices to your computer.

volume – A hard or floppy disk, partition of a hard disk, Subvolume, file server, or any data storage medium that is logically recognized by Retrospect as a file and folder storage location.

INDEX

B

C

D

E

F

60 slots, and you specify a maximum of 15 slots per magazine, Retrospect creates four magazine containers with 15 slots each. The number you specify does not represent any actual physical grouping of slots or magazines; it is for display purposes only.

If your tape library supports barcode reading, Retrospect automatically uses barcode data to generate the information displayed in the Storage Devices window. You can disable barcode scans by clicking the Disable/Enable Barcode Scans button 🏷. You can also click the Clear Barcode Information button 🏷 to unlink barcode information from all known tapes. This feature should only be used if Retrospect is incorrectly displaying barcode information or tape names, or if directed to do so by Tqzkq Retrospect Technical Support.

Add to Backup Set lets you add tapes in the selected slots as members of a tape Backup Set. See "Preparing Tapes for Use" on page 44 for more information.

Scan Selected cycles through the selected storage slots in the library, moving each tape from slot to drive to learn the name of the tape. You do not need to use this command if your tape drive supports barcodes.

Erase Selected erases each tape in the selected storage slots of the library.

NOTE: If your selection includes WORM tapes, Retrospect skips them when erasing.

Move Selected to Drive moves the selected tapes from their slots to the tape drive(s).

Unload All/Eject Magazine unloads tapes from the library's drive(s) and returns them to their slots. Then, for capable libraries, ejects the library's magazines.

Cleaning Slot designates the selected slot as a cleaning slot. Retrospect will not scan the cleaning slot when it searches for media. If your

library supports barcode reading, Retrospect automatically recognizes a CLN-coded cleaning tape and reserves its slot for cleaning purposes. You can specify the number of cleanings per tape and how often to clean a tape drive from the Properties window for the drive or tape. See "Cleaning Your Tape Drive" on page 42.

Initialize Elements sends the Initialize Element Status command to the library, which forces the library to update the status of all elements. Use this command if you encounter a situation in which the information reported in the Storage Devices window does not match the actual state of the library.

Import-Export Support

Some libraries come with separate ports that are used to load single tapes into and from the library without opening the door. Retrospect uses the term "import-export slot" for this feature, which is also known as "Mail Slot," "I/E element," and "Call Slot." If the import-export slots are present and enabled in a library, Retrospect displays them as separate slots at the top of the list of slots. You can drag and drop tapes from the source drive or any slot onto the import-export slot and the library will move the selected tape to the port. When you place a tape into the port, Retrospect displays "Media Available" next to the import-export slot and you can move it by dragging it to any slot or drive in the library.

Retrospect does not scan import-export slots during unattended operation. Do not place a tape in the import-export slot if you want to use the tape in an unattended operation such as a scripted backup.

Tape Library Media Requests

During immediate and automated operations, Retrospect scans the library, searching for the appropriate media, and loads whichever tape is required. If a new or erased tape is required,