Retrospect® 8

User's Guide

Retrospect 8 Users Guide, first edition.

Table of Contents

Chapter 1: Introducing Retrospect 8

Welcome to Retrospect 8! This chapter first describes the different editions of Retrospect, then defines the program's hardware and system requirements. Next, you'll see how to install Retrospect's components, and how to upgrade from previous versions of Retrospect. Finally, there's a basic overview of Retrospect's console, which is the user interface you'll be working with the most.

Overview of Retrospect

To backup and restore data, Retrospect uses three software programs:

The *Retrospect engine* is the backup and restore software running on the *Retrospect server,* which is the computer that has the storage devices attached to it. The Retrospect engine runs in the background on the Retrospect server. If you have more than one Retrospect license, you can control multiple Retrospect servers from a single user interface.

The *Retrospect console,* also called the Retrospect application, provides the user interface with which you control the functions of the program. You'll use this to create immediate or scripted backups; restore backed up files and folders; monitor running backup and restore activities; get reports of recent and scheduled activities; and much more. The Retrospect console doesn't have to be installed on the same computer as the Retrospect engine. If you have a larger installation with more than one Retrospect server on your network, you can administer all activities on each server from a single Retrospect console.

The *Retrospect Client software* must be installed on every computer on your network (Mac, Windows, or Linux) that you wish to back up to the Retrospect server. The Client software allows Retrospect to copy and restore data across the network, as though the client computers' drives were connected directly to the Retrospect server.

Which Edition Is Right for You?

Retrospect is licensed in four main ways:

- **Desktop 3-User** backs up a single machine and two clients (Mac, Windows, or Linux), and it includes open file backup for Windows XP and Vista clients. This license will not back up a server, such as Mac OS X Server or Windows Server, and is limited to a single activity thread.
- **Single Server 20 Clients** is for small networks with moderate backup and restore needs. A Single Server license will back up one Mac OS X Server or Windows Server and up to 20 clients.

- **Single Server Unlimited Clients** will back up one Mac OS X Server or Windows Server and any number of clients.
- **Multi Server Unlimited Clients** is for larger installations that need to protect multiple Mac OS X Servers or Windows Servers and any number of clients.

Retrospect Add-On Products

A number of advanced Retrospect features are only available if you have the appropriate license code. To view your current licenses, or to purchase additional licenses, choose Retrospect > Preferences, then click the Licenses tab.

Advanced Tape Support

The Advanced Tape Support add-on improves overall backup times to tape libraries and autoloaders by utilizing multiple tape drives in parallel, including stand-alone drives, drives in libraries, or drives in autoloaders. 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. This add-on is not required for the following tape support features, which are already built into the Retrospect product: support for barcodes and cleaning tapes, sequential use of tape drives, and multiple simultaneous operations when backing up to hard drives.

Open File Backup for Windows Clients

The Open File Backup add-on protects files (on NTFS file systems) that are open and in use on Windows servers, desktops, and notebooks. It protects files on multiple volumes as well as business-critical server applications that run 24 hours a day including e-mail, database, CRM, accounting, or proprietary applications. For desktop and notebook computers, backups can take place while e-mail applications and other applications are in use. A single Open File Backup add-on license protects all networked Windows computers backed up by a single Retrospect server.

Server Client Licenses

Server client licenses are available to back up networked servers. Server client licenses can be purchased for use with both Single Server editions. (Retrospect Multi Server edition is licensed to protect an unlimited number of networked servers.)

Retrospect Clients

Retrospect uses client software to provide fast backups of networked Macintosh, Windows, and Linux computers. All editions of Retrospect for the Mac can be expanded with the purchase of client packs (licenses) that protect additional networked client computers. Client packs are installed on the Retrospect server and are available for 1, 5, and 10 client computers.

The Retrospect Client software must be installed on each client computer to be protected. Client installers are available from the Retrospect product CD or can be downloaded from the Updates page in the Support section of the Retrospect website.

Requirements

Retrospect 8 engine

Dual-processor PowerPC G4, PowerPC G5, or any Intel processor
Mac OS X 10.4.11 or 10.5.5 or later
At least 2 GB RAM
10-15 GB of hard disk space for each concurrent activity
Storage for backups

Retrospect 8 console

PowerPC G4, G5, or any Intel processor
Mac OS X 10.5.5 or later
At least 2 GB RAM
50 MB hard disk space

Retrospect 8 Client Software

Mac OS X

PowerPC G3, G4, or G5, or any Intel processor
Mac OS X or Mac OS X Server 10.3.9, 10.4.11, or 10.5.5 or later
RAM that meets Apple's guidelines for each OS

Windows

Pentium processor or later
Windows 2000, XP, Vista, or 7; Windows 2000 Server, Windows Server 2003 or 2008
RAM that meets Microsoft's guidelines for each OS

Linux

x86-based system running Red Hat Linux, Red Hat Enterprise Linux, SUSE Linux Desktop, SUSE Linux Professional, SUSE Linux Standard Server, or SUSE Enterprise Server operating system.
glibc version 2 or later
In order to use the graphical user interface (GUI) to change options and preferences, Java version 1.2 or later is also required.

Note: For a current list of supported versions of Red Hat Linux, SUSE Linux and other Linux distributions, see the Retrospect website.

Storage Devices

Retrospect supports a wide variety of storage devices as the destination for your backups, including hard drives (both direct- and network-attached), tape drives and libraries (connected via FireWire, SCSI, iSCSI, Fibre Channel), and removable disk drives See the Retrospect Support website for a complete list of supported tape drives and libraries.

`http://www.retrospect.com/supporteddevices/`

Installing Retrospect

To install Retrospect, you need to install three separate software programs:

- On the *Retrospect server* (i.e., the machine that will be performing the backups on your network, and that has backup storage devices attached), you must install the *Retrospect engine.*
- On one or more machines that will be administering Retrospect, you must install the *Retrospect console.* A single console can control one or more Retrospect servers.
- On each machine on the network you want to back up with Retrospect, you must install the *Retrospect Client software.* There are Retrospect Client installers for Mac OS X, Windows, Linux.

Note for upgraders: Retrospect 8 will coexist on machines that have Retrospect 6.1 installed, and will not interfere with operations of the older software.

Installing the Retrospect Engine

To install the Retrospect engine:

1. On the machine you want to make the Retrospect server, insert the Retrospect CD or double-click the downloaded disk image to mount it on your desktop.
2. Double-click Install Retrospect Engine.
3. When prompted by the Installer, enter an administrator's username and password, then click OK.
4. Follow the Installer's instructions.

Installing the Retrospect Console

To install the Retrospect console:

1. On the machine you want to use to administer the Retrospect server, insert the Retrospect CD or double-click the downloaded disk image to mount it on your desktop.

2. Drag the Retrospect 8 Management Console folder icon to copy it to your Applications folder. In the Retrospect disk image, there is an alias to the Applications folder to make this easier.

Installing Retrospect Client software on a machine running Mac OS X

Note: To install the Retrospect Client software using the public/private key authentication method, which provides additional security and allows the Retrospect server to automatically connect to clients with the matching public encryption key, refer to Chapter 4: Working with Clients, Servers, and Network Shares.

1. On each machine you want to backup over the network to a Retrospect server, insert the Retrospect CD or double-click the downloaded disk image to mount it on your desktop.
2. Double-click the Client Installers folder to open it, then double-click to open the Mac Client Installer folder. Finally, double-click Install OS X Client.
3. When prompted by the Installer, enter an administrator's username and password, then click OK.
4. Follow the installer program's instructions.

Installing Retrospect Client software on a machine running Microsoft Windows

Note: To install the Retrospect Client software using the public/private key authentication method, which provides additional security and allows the Retrospect server to automatically connect to clients with the matching public encryption key, refer to Chapter 4: Working with Clients, Servers, and Network Shares.

1. On each machine you want to backup with Retrospect, copy the Windows Client Installer folder found inside the Client Installers folder on the Retrospect CD or downloaded disk image to the

Windows desktop.

2. Open the Windows Client Installer folder.
3. Double-click *Retrospect Client for Windows [version number].exe*, then follow the program's instructions.
4. If requested, restart the Windows client machine.

Installing Retrospect Client software on a machine running Linux

1. On each machine you want to backup with Retrospect, insert the Retrospect CD or double-click the downloaded disk image to mount it on your Macintosh desktop.
2. Double-click the Client Installers folder to open it, then double-click to open the Linux Client Installer folder. Inside, you'll find the Retrospect Client for Linux installer files (*Linux_Client_[version number].rpm or Linux_Client_[version number].tar*).
3. Copy the appropriate file to a location on the network, then copy the file to the Linux computer on which you want to install the client software.
4. Save all unsaved documents in other running application programs.
5. Enter the following commands, depending on your operating system and your preferred installer.
6. `rpm $rpm -i Linux_Client_7_6_100.rpm`

   or

   `tar $tar -xf Linux_Client_7_6_100.tar, $.Install.sh`
7. 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 clients. Macintosh high-bit characters do not correspond to Windows high-bit characters. For example, Luf$Luf00 is okay but Lüf•Lüføø will cause problems.*

The client software runs automatically upon completion of installation.

Upgrading from Previous Versions of Retrospect

Because Retrospect 8 for Mac has a different underlying architecture and uses different configuration files than previous versions of Retrospect for Mac, version 8 does not import settings from version 6.x or earlier installations. When upgrading, it is therefore necessary to rebuild the backup environment in Retrospect 8. The general steps to take are as follows, along with the chapters in which these steps are covered in this Users Guide.

1. Install Retrospect 8 server and console (Chapter 1); configure preferences (Chapter 7).
2. Create new Media Sets and assign media to contain the backup data (Chapter 5).
3. Create new Rules (which replace Selectors from previous versions) (Chapter 7).
4. Log in Retrospect client computers and network shares (Chapter 4).
5. Define Favorite Folders, which replace subvolumes from previous versions (Chapter 3).
6. Assign tags, which replace Source Groups from previous versions (Chapter 3).
7. Create scripts for backup, copy, grooming, etc. operations (Chapters 5 and 7).

Stopping and Starting the Retrospect Engine

After you install the Retrospect engine on the Retrospect server machine, it automatically starts, and you should not normally need to interact with it other than by using the Retrospect console. However, if you want to manually shut down the engine, you may do so.

1. On the Retrospect server machine, open System Preferences.
2. In System Preferences, click the Retrospect icon.
3. Click the padlock icon in the lower left corner of the window. Enter an administrator's name and password and click OK.
4. To shut down the engine, click Stop Retrospect Engine. After a moment, the engine stops, and the button changes to Start Retrospect Engine. Click the button again to restart the engine.
5. Normally, the Retrospect engine automatically starts upon system startup. If you do not want this to occur, uncheck "Launch Retrospect Engine on System Startup."

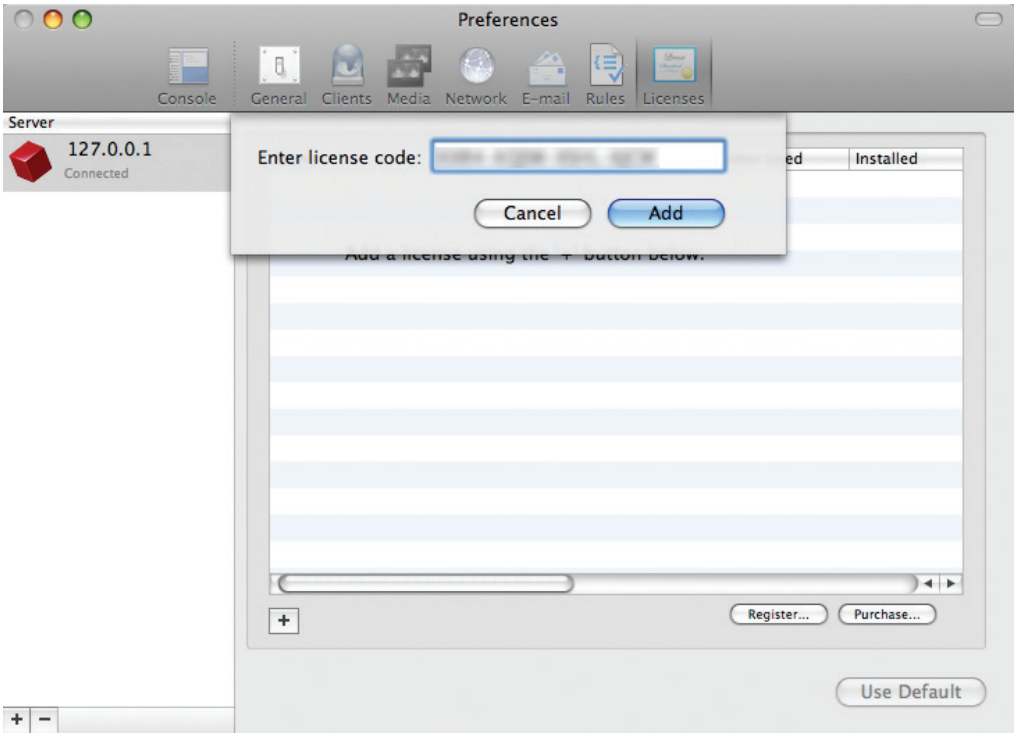
Starting and Stopping the Retrospect Console

To start the Retrospect console, double-click the Retrospect application icon inside the Applications folder on your machine. The Retrospect console will open and automatically look for a Retrospect engine running on the same computer. If one is present and running, the Retrospect console will connect automatically. If a local Retrospect engine is not present, you may add one or more remote Retrospect engines by clicking the plus (+) button in the bottom bar of the console.

Tip: *In the Server Address of the resulting dialog, you may enter the IP address of the machine with the running Retrospect engine, or, if the machine is on your local subnet, you may enter its Computer Name, for example, Server.local. You can find a machine's Computer Name in the Sharing category of its System Preferences.*

The first time you connect to a local or remote Retrospect engine, Retrospect opens its Preferences window and asks you to enter your license code for that

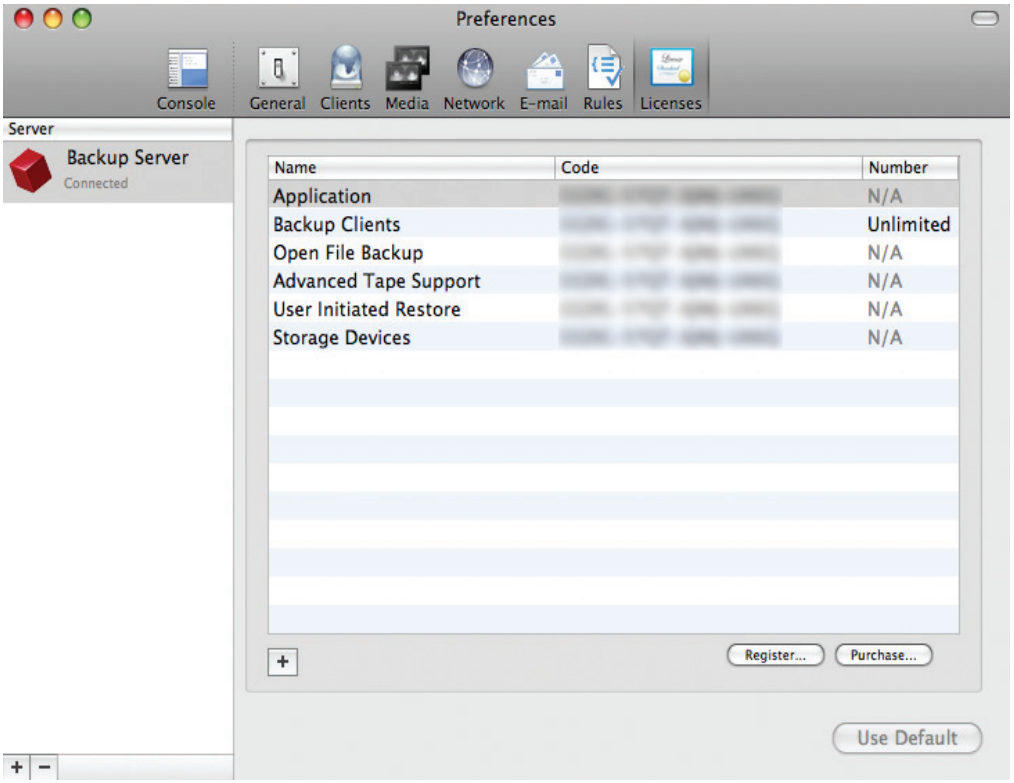
engine. Enter this information, then click Add.



At the registration screen prompt, click one of the following buttons:

- **Register,** if you have not registered your copy of Retrospect and would like to do so. Clicking this button will launch your default Web browser and take you to the registration website, where you can fill out a registration form.
- **Already Registered,** if you have already registered your copy of Retrospect.

Depending on the license code you entered, the Licenses pane of Retrospect Preferences will show the codes for the Application, Backup Clients, or Storage Devices.



Tip: *While the Preferences window is still open, we suggest that you take a moment to click on the General pane, and enter a name for the Retrospect server in the Server name field. By default, Retrospect uses the server machine's Computer Name as shown in System Preferences' Sharing panel as the server name, which may not be as descriptive to you and your users as you would prefer.*

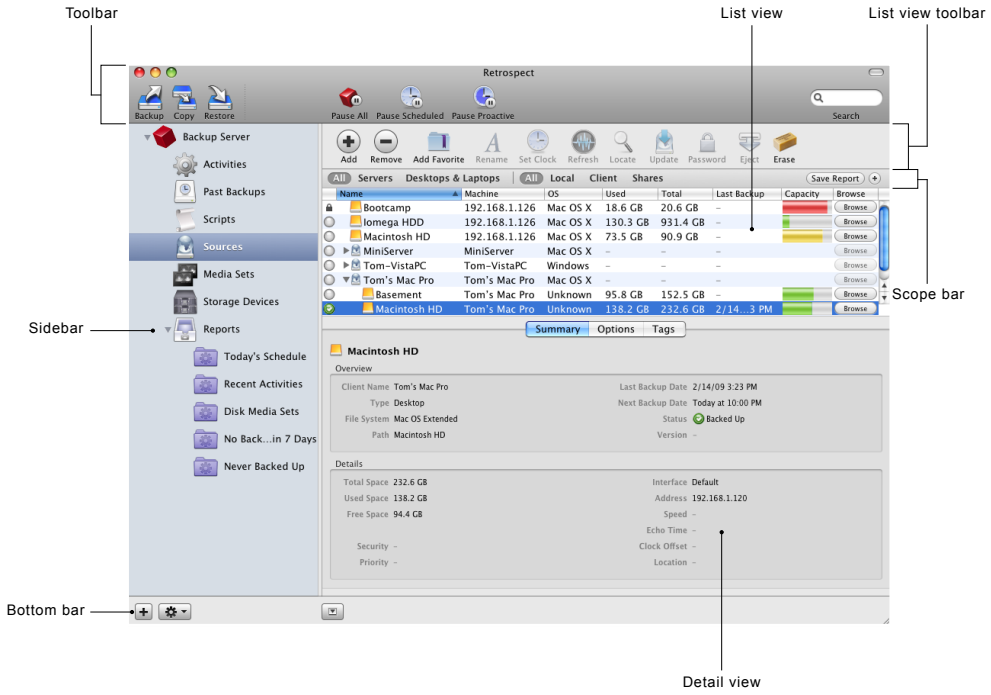
You should also assign a password for each Retrospect engine you logged in by clicking the "Change server password" button and entering a password of your choice. This step prevents unauthorized access of the Retrospect engine from other Retrospect console applications running on your network.

When you're done with the Preferences window, click its close box to dismiss it.

To exit Retrospect, choose Quit Retrospect from the Retrospect menu, or press Cmd-Q.

Overview of the Retrospect Console

The Retrospect 8 console is the user interface that controls actions that occur on the Retrospect server. The Retrospect console can be running on the Retrospect server machine, or it can operate the server from elsewhere on the network. Let's take a detailed look at the console window.



The Retrospect 8 console window is made up of several sections:

Toolbar

The toolbar across the top of the window contains buttons to launch the Backup, Copy, and Restore Assistants (these are the easiest way to create scripts and perform activities in Retrospect), the pause activity buttons, and the Search Field.

Sidebar

The sidebar on the left is where you choose which Retrospect server to control. If you have multiple Retrospect servers on your network, all of them will appear in the sidebar. Click on the disclosure triangle next to a server to show or hide its items, which allow you to control the functions of that server. Each server has the following items:

- **Activities** shows a list of the backup, copy, and restore events that Retrospect has performed, is performing, or is scheduled to perform (depending on your choice from the scope bar). Status icons in the left-most column show if the activity was successful or had problems. You can also tell the date and time of the activity; the name of the script associated with the activity; the type of operation; the activity's sources and destinations; and (for current and past operations) the speed of the activity.
- **Past Backups** combine previous versions of Retrospect's concepts of Snapshots (the listing of all files present on a source volume during a backup) and sessions (the actual files copied during a backup operation). You can filter the list of past backups by Mac or Windows clients.
- **Scripts** control all actions in Retrospect, either with or without a schedule. The concept of immediate actions without creating a script (like an immediate backup) no longer exists. Any script can be run immediately by highlighting a script in the Scripts list and clicking the Run button in the list view toolbar.

  You can explore and modify a selected script using the detail view below the Scripts list. By clicking on the tabs in the detail view, you can view a summary of the script; set the script's source, destination, and rules; create or modify a schedule for the script to run; and set various script options.
- **Sources** displays a list of all local volumes and logged-in network shares for the Retrospect server, and added Retrospect client computers. You may add any client computers running the 6.1 (or later) Retrospect Client for Mac or the 7.6 (or later) Retrospect Client for Windows by clicking the Add button in the list view toolbar of the

Sources list view. NAS devices and shares can be added similarly. The Sources list gives you information about each Source, including its name, the machine it resides on, the OS that machine is running, its capacity and how much of that capacity is used.

- **Media Sets** shows you a list of the Media Sets used for backups. Using the scope bar, you can filter the results of the list by the different Media Set types: All, Tape, Disk, and File.
- **Storage Devices** shows a list of the storage devices attached to the Retrospect server. This list does not display hard disks, removable disks, or NAS volumes (those are shown under Sources); rather, it includes hardware devices such as optical and tape drives and libraries.
- **Reports** are the last item in the sidebar. Click the disclosure triangle to view the list of included reports. Custom reports can be saved from nearly any list view. Right-click any of the column headings in a list view to show or hide specific columns you want to appear in the report, click the column heading to set the sort order, click scope buttons to filter the results shown in the list, click the plus (+) button at the right of the scope bar to add further filter conditions, drag conditions if needed to change their order, then click Save Report in the scope bar. You'll be asked to name the report. Any reports that you create will appear at the bottom of the Reports list.

List and Detail Views

The list view and an optional details view are in the main section of the window. The list and detail contents change depending on the item selected in the sidebar, and on choices made in the scope bar.

List View Toolbar

The list view toolbar beneath the main toolbar displays a variety of context-sensitive buttons based on the selected item in the sidebar.

Scope Bar

The scope bar has context-sensitive scope buttons, the Save Report button, and the (+) add condition button which appears above the list view when

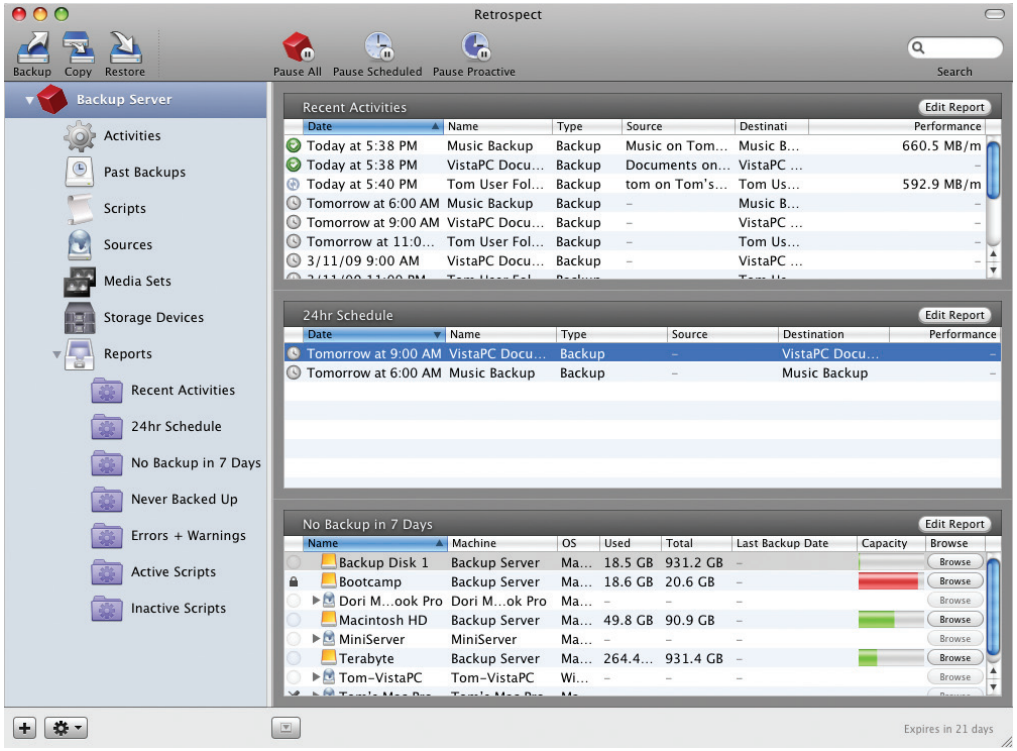
appropriate and allows you to filter the list view based on pre- and user-defined conditions.

Bottom Bar

The bottom bar contains the (+) add button to add a Retrospect server to the sidebar, the gear icon Action menu button (which allows you to edit reports and pause operations) and the show/hide button for the details pane.

Dashboard

The Dashboard only appears when you click on a Retrospect server in the sidebar. It contains an overview of selected Reports for that server, presented in one handy view. You can use the Dashboard to get a quick summary of your all of your backup, copy, and restore activities. Any report can be added to the Dashboard view.



Chapter 2: Fundamentals

This chapter describes Retrospect's main concepts. This manual and the program itself refers constantly to these basic ideas, so it is important to understand them to get the most out of using Retrospect. In this chapter, you'll learn how Retrospect works; about the different kinds of Media Sets you can use to back up your data; and about the backup actions you can take with Media Sets.

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 backup media indefinitely. For example, if you have been working on a particular document over a period of time, Retrospect backs up a different version of the document each time you back up. If necessary, Retrospect lets you retrieve a previous version of the file from any point in time it was backed up.

Retrospect always performs Smart Incremental backups. A Smart Incremental backup intelligently copies only files that aren't already present on the current Media Set being used for backups (typically those files that are new or have changed since the previous backup). You don't have to specify whether you want a "full" or "incremental" backup. Retrospect, by default, copies any and all of the files it hasn't already backed up.

Because Retrospect only needs to add one instance of each unique file to the backup, it saves space on the backup media that would otherwise be used up storing duplicate copies of files. This space-saving technique is known as *file-level deduplication* or *single-instance storage*.

All of the backup, copy, and restore operations in Retrospect require a source and a destination. For a backup, the source is generally a hard drive or a folder on a hard drive (Retrospect calls these sources and Favorite Folders, respectively). The destination is generally a Media Set stored on backup media such as disk or tape.

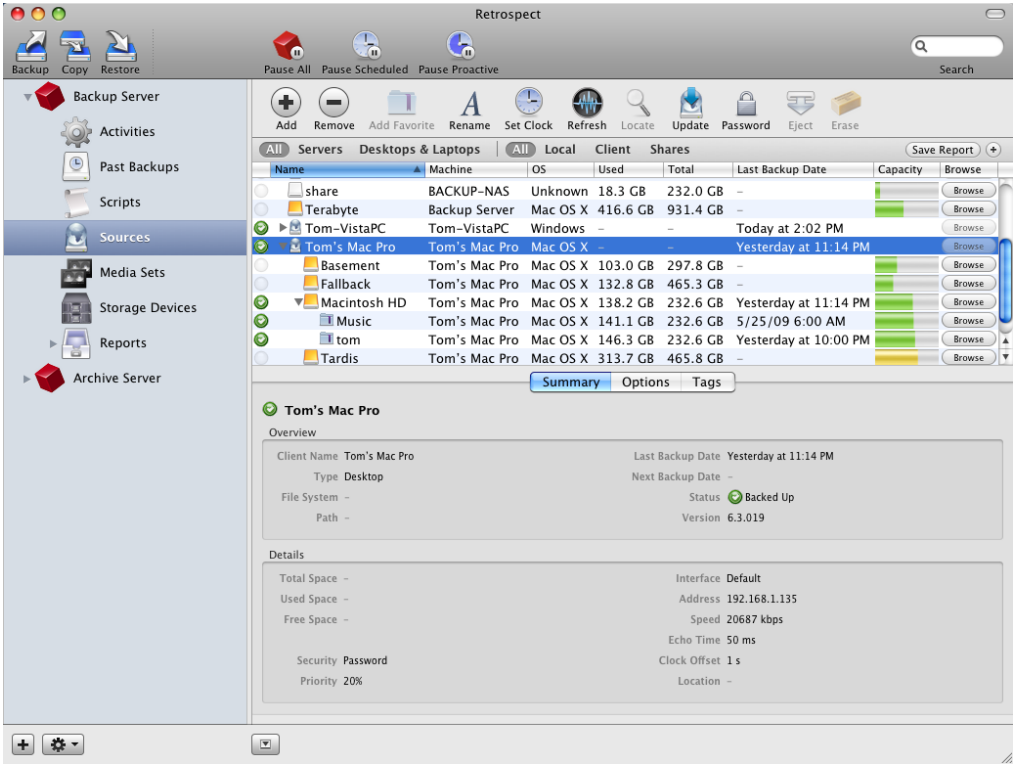
Retrospect uses a Catalog file, an index of the files and folders contained in a Media Set, to keep track of the different generations of modified files in a Media Set. The Catalog lets you quickly search for files without having to actually search the backup media itself, which would be considerably slower, especially with media like digital tape. By default, Catalog files are stored on the Retrospect server computer, in

`Library/Application Support/Retrospect/Catalogs/`.

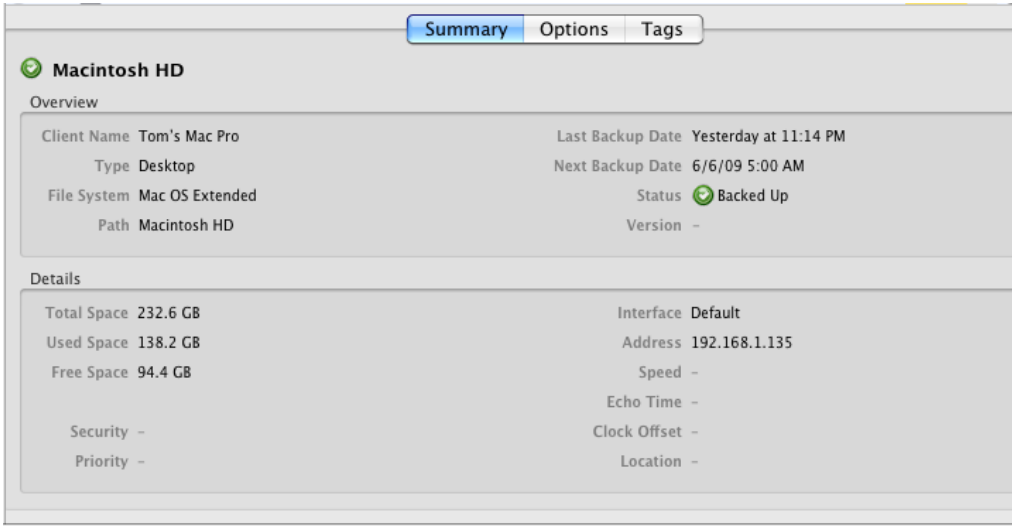
Sources

Sources are the disk volumes, folders on disk volumes, and networked clients that you want to back up. Each source you want to back up needs to be added to the Sources list.

It’s important to understand that Retrospect uses the term sources to refer to the volumes and folders that you want to back up, and also to refer to hard disk volumes that those backups will be written to. For example, you can back up a client’s hard disk called My Disk (that’s a source) to a Disk or File Media Set that resides on a hard disk named Backup Disk (because it is a hard disk that could also be backed up, Backup Disk also appears in the Sources list).



Above the Sources list, the toolbar allows you to add or remove sources, add Favorite Folders, and otherwise work with items in the Sources list. Below the list, a tabbed area allows you to see important details on a source that you have selected in the list.

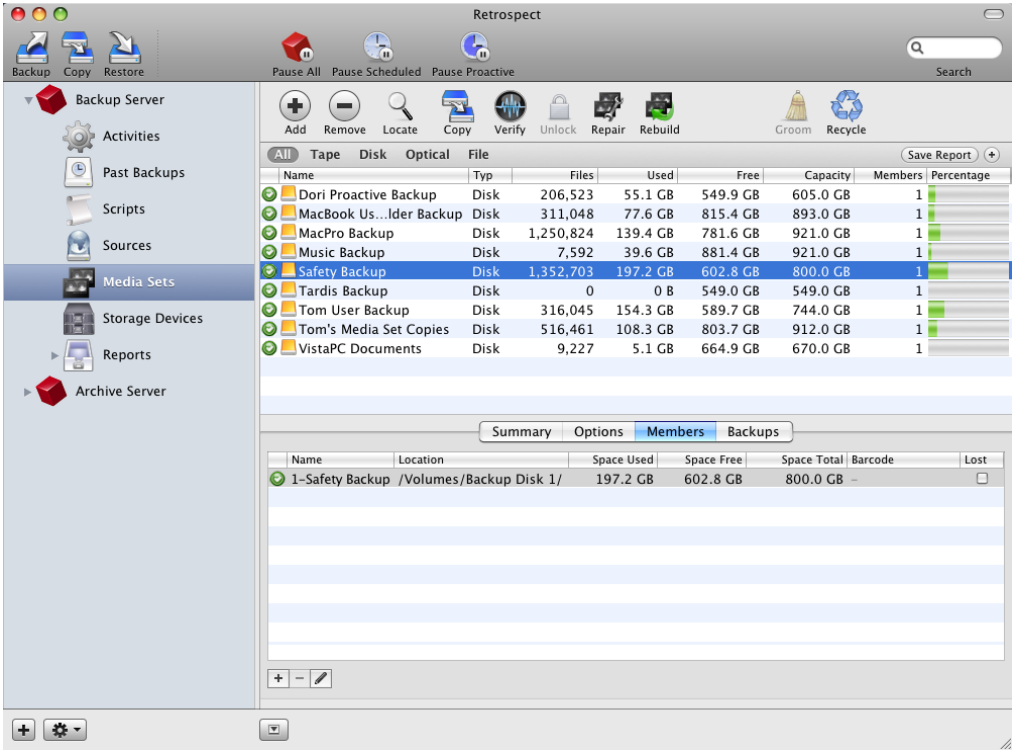


Media Sets

Media Sets are the destinations for files and folders that you back up. A Media Set consists of one or more disks, tapes, optical discs, or a single file. Individual pieces of media (for example, tapes, optical discs, or hard disks) are members of a Media Set. A Media Set consists of one or more disks or tapes, or a single file. Individual pieces of media (for example, tapes or hard disks) are members of a Media Set. A Media Set can be made up of almost any sort of storage media: hard drives, disk arrays, tape, and even flash memory.

You can backup as many source volumes as you like to a single Media Set. For example, you could have a single Media Set as the backup destination for your computer's internal hard disk, your external hard disk, a coworker's hard disk on a computer with installed Retrospect Client software, and even a Mac OS X Server or Windows Server. All of your Media Sets appear in Retrospect's Media Sets list.

Above the list, the toolbar allows you to work with Media Sets, including functions such as adding, removing, copying, and verifying a Media Set. Below the list, tabs give you more information on the Media Set you have selected.



When a disk or tape fills with data, Retrospect asks for a new member, adds it to the Media Set and continues appending data. It automatically uses any available new or erased media. If the media has the name Retrospect is looking for, Retrospect will erase and reuse it. However, Retrospect will never automatically use a medium with the wrong name if it has data on it.

When you create a Media Set in Retrospect, it can be one of the following types:

- **Disk Media Sets** are Retrospect's most flexible Media Set. They allow backups to span across multiple, random-access storage devices, including hard disks, Network Attached Storage (NAS), removable cartridges, and even flash media. Older backups can be groomed from Disk Media Sets to reclaim space, and it's even possible to perform a restore from a Disk Media Set that's in use by a backup operation. Disk Media Sets should be your most-used backup destination if you

are not using tape backup. A Disk Media Set writes a folder containing a series of files to the destination media, with each file being no larger than 600 MB (which can be useful in environments where these files are replicated to additional storage, such as an off-site vault). Retrospect considers the folder containing the backup files to be a single member of the Disk Media Set. Disk Media Sets replace the less-flexible Removable Disk sets present in older versions of Retrospect. Catalogs for Disk Media Sets are usually stored on the Retrospect server's hard drive.

- **Tape Media Sets** use tape drives and backup tapes as the storage medium. Retrospect supports many types of tape drives, including DAT drives, LTO drives, AIT drives, VXA drives, and DLT drives. See the Retrospect website for a complete list of supported drives. Some drives, such as tape libraries (which can accommodate and automatically load multiple tapes) may require a license for the Advanced Tape Support add-on. Catalogs for Tape Media Sets are usually stored on the Retrospect server's hard drive.
- **Tape WORM Media Sets** are similar to Tape Media Sets, except that the tapes they use are WORM (Write Once, Read Many). As the name suggests, WORM tapes cannot be erased or reused once data is written to them. They are used for archival purposes and to comply with government regulations requiring document retention. Catalogs for Tape WORM Media Sets are usually stored on the Retrospect server's hard drive.
- **File Media Sets** combine the Catalog file and the backed-up data into a single file stored on a volume. They can be saved anywhere a Disk Media Set can be saved, but they are limited by the size of the volume on which it is stored, and also the maximum file size of the file system (FAT32, NTFS, HFS+, etc.). Backups in a File Media Set cannot span across media. File Media Sets are useful for small jobs where everything (the Catalog and the backed up data) is self-contained in a single file, but in most cases, you should use Disk Media Sets.

Media Actions

Whenever you run a backup script manually, or when you set a script to later run automatically, you have the option of using one of four media actions. Each media action tells Retrospect how to handle the physical media, which in turn has an effect on which files are backed up.

Retrospect's four media actions are:

- **No media action**, which is the default choice, tells Retrospect that it doesn't need to do anything special with media during the current backup. As usual, Retrospect will perform a Smart Incremental backup, which saves time and media space by not copying files that already exist in the Media Set. In other words, Retrospect will copy only files which are new or newly modified since the last backup to the same Media Set.
- **Skip to new member** causes Retrospect to create a new member within the current Media Set. Retrospect will display a dialog requesting a new piece of media, so that you can insert it for use in the next backup operation. This media action is useful when a piece of media that you have previously used for a particular Media Set is not available.
- **Start new Media Set** tells Retrospect to create a new destination Media Set (with a name similar to the old one) of the chosen type. Depending on the type of Media Set, Retrospect will use a new or erased disk or tape. For Disk Media Sets, Retrospect will create a new folder on the disk, and backed-up data will be written as a series of 600 MB backup files inside that folder. Use the Start new Media Set media action so that you can take your old media off-site for safe storage.
- **Recycle Media Set** first clears the catalog contents (if any) of the destination Media Set, so it appears no files are backed up. Then it looks for the first media member of the Media set and erases it if it is available. If the first member is not available, Retrospect uses any available new or erased piece of media appropriate for the Media Set type. All selected files and folders from the source are then backed up to the Media Set. Use the Recycle Media Set action when you want to reuse one or more pieces of media.

Note: As long as matching is left on (the default), Retrospect will always perform a Smart Incremental backup, adding only those files that don't exactly match already-backed-up files. If a Media Set and its catalog file are empty, then Retrospect's Smart Incremental backup will automatically add all the files necessary to restore each backed-up source.

Catalog Files

Retrospect uses a separate catalog file (usually stored in `/Library/Application Support/Retrospect/` on the Retrospect server) to keep track of all of the files and folders in a Media Set. You can think of the catalog as an index or table of contents of the files on the backup media. The catalog lets you view the contents of a Media Set without requiring the media to be inserted in the backup device, greatly speeding up finding and retrieving files.

A catalog file is required for all operations that copy files to and from a Media Set. Retrospect can repair damaged catalogs, using the Repair button in the list view toolbar under Media Sets. If the catalog is lost or damaged too severely for the repair operation, Retrospect can rebuild it by reading and reindexing the media.

Retrospect Clients

Retrospect can back up any drive that can be mounted on the Macintosh desktop, whether that drive is local or a shared networked volume.

Retrospect Clients extend the backup and restore capabilities of Retrospect to other computers on your network. A computer equipped with the 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, and it does so with full administrator privileges on those systems.

Proactive Backups

Retrospect's Proactive Backups accommodate changing network and disk configurations.

A Proactive Backup offers a special type of scripted backup. Rather than backing up sources on specified days and/or times to specified Media Sets (like a traditional script), Proactive Backup scripts look for transient computers and volumes, such as notebook computers with the Retrospect Client software installed, to appear on the network. When the sources appear, Retrospect backs them up. Retrospect Client users can even request backups of their volumes. A Proactive Backup script is often best used in concert with regular backup scripts to produce a comprehensive backup strategy.

Chapter 3: Hardware

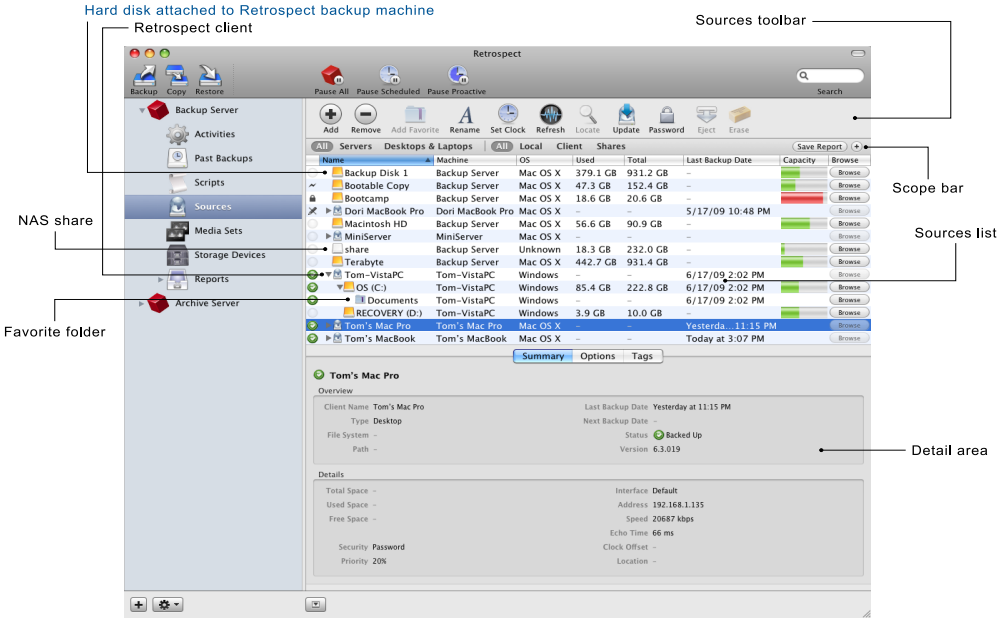
This chapter explains how Retrospect works with your different backup devices, and explains how you can see and control your hardware from within Retrospect.

Sources and Storage Devices

Retrospect displays your hardware in two different areas of the program, Sources and Storage Devices, accessible from the sidebar.

Sources

The first area, Sources, shows you the hard drives that are attached to the computer running the Retrospect backup engine, and on those hard drives, shows you any Favorite Folders that you have defined. Retrospect treats Favorite Folders as separate sources that can be backed up independently of the hard drive on which they reside. Sources also shows you the network volumes that you tell Retrospect about. These can either be mounted network shares, such as on a file server or NAS (Network Attached Storage) device, or Retrospect clients (computers running the Retrospect Client software). See Chapter 4 for more information about working with Retrospect clients, NAS devices, and network shares.



Retrospect uses different icons in the Sources list to display each of the different types of Sources.

Hard drive; may be connected to Retrospect server machine or be attached to a Retrospect client machine.

Retrospect client; shown here with disclosure triangle, indicating that it can be opened to display the hard drives attached to the Retrospect client machine.

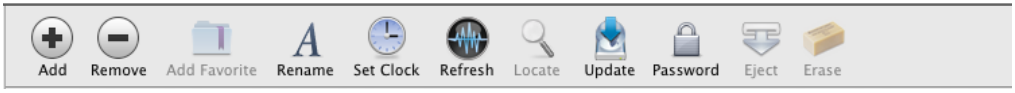
A network volume or share logged in using a file sharing protocol, such as AFP or SMB.

Favorite Folder.

Retrospect has the ability to use any kind of media that can be mounted on the Mac desktop as a source. So it doesn't matter whether the media is a hard drive, a network share, a Retrospect client machine with attached hard drives, or even devices such as flash memory drives or disk drives with removable media, all of these will appear in the Sources list.

Using the Sources toolbar

Above the Sources list, the Sources toolbar allows you to perform various actions on an item selected in the Sources list. Depending on the selected Source, different items in the toolbar may or may not be active.



The buttons in the toolbar have the following functions:

- **Add** opens a dialog that allows you to add a network share or Retrospect client computer to the Sources list.
- **Remove** allows you to remove a selected Retrospect client computer, network share, or Favorites Folder from the Sources list.

- **Add Favorite** allows you to choose and designate a folder on a selected Source as a Favorite Folder.
- **Rename** allows you to rename the selected Retrospect client. This changes the client name in Retrospect, but it does not change the actual machine name. In other words, it only changes the client name as it appears in the Retrospect Sources list.
- **Set Clock** changes the time and date on the selected Retrospect client computer to match the date and time on the Retrospect server.
- **Refresh** tests the connection to the selected Retrospect client computer and updates details such as IP address and connection speed.
- **Locate** lets you associate an existing Retrospect client with a new address without removing that client from any scripts.
- **Update** allows you to update the Retrospect Client software on the selected computer.
- **Password** changes the login for the selected network share or Retrospect client computer.
- **Eject** unmounts the selected network share.
- **Erase** will erase all data from the selected source. You should be very careful when using this, as this operation cannot be undone.

Using the Scope bar

Because the number of Sources you are managing with Retrospect can be very large, the Scope bar allows you to filter the items in the Sources list in two fashions. To filter the Sources shown in the list, click one of the buttons in the Scope bar.

The first group allows you to filter the items in the Sources list by the operating system used by the Source.

Clicking the Servers button restricts the list only to computers running a server operating system. This includes any versions of Mac OS X Server,

Windows Server, and server software used by NAS (Network Attached Storage) devices. Clicking the Desktops & Laptops button filters the list to show only Retrospect client computers running a non-server operating system supported by Retrospect (see Requirements in Chapter 1 for a complete list).

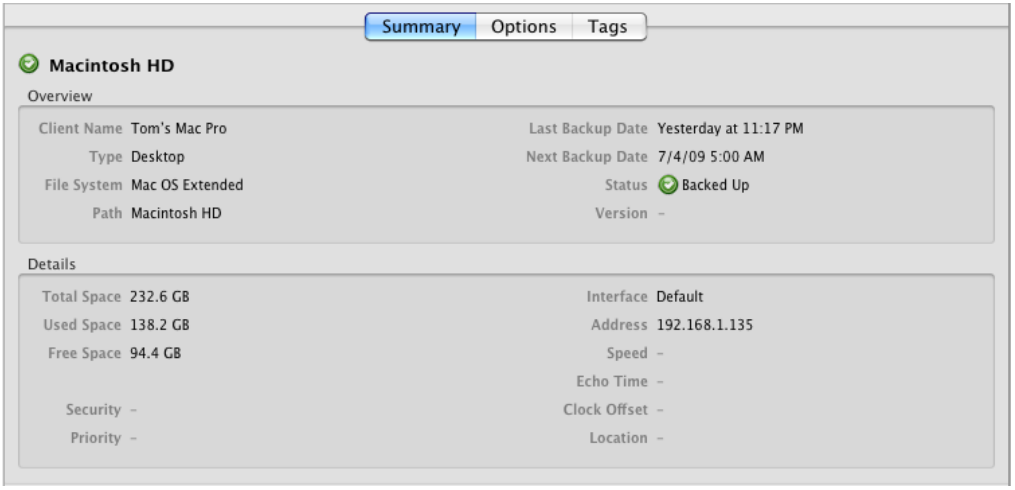
The second group allows you to filter the items in the Sources list by type. Clicking the Local button shows you Sources connected to the Retrospect server computer. Clicking the Client button shows you only the Retrospect client computers. Clicking the Shares button shows you only network shares.

Note: The two groups of buttons in the Scope bar are interactive, and clicking buttons in the first group of the Scope bar will affect items shown when you further filter the results in the second group. For example, imagine that you have a NAS device attached to your network. If the selected filter in the first group is All or Servers, clicking Shares in the second group will still display the NAS. But if the Desktops & Laptops button was selected in the first group, that would filter out the NAS, and no selection in the second group would display the device.

Using the Detail area

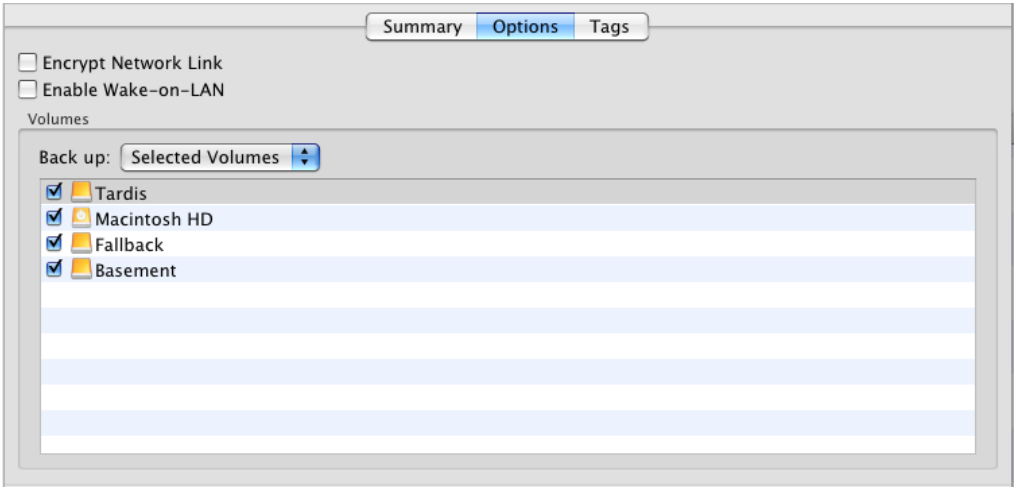
Below the Sources list, the Detail area shows additional information about whichever Source is selected in the Sources list. There are three tabs in the Detail area: Summary, Options, and Tags.

Summary: In the Summary tab, Retrospect shows you information about the selected Source, and that information changes depending on the kind of Source you have selected.



The Overview section tells you the key information about the Source, including the Client's name, its last and next scheduled backup dates, and its backup status. The Details section displays information about the Source's capacity, its network address information, and its backup performance speed.

Options: In the Options tab, the items are only active for Retrospect client machines.



Check the box next to Encrypt Network Link to encrypt data transfers between the selected Retrospect client computer and the Retrospect server. Check the

box next to Enable Wake-on-LAN if you want to make sure that Retrospect wakes up a sleeping client computer for Proactive Backup activities.

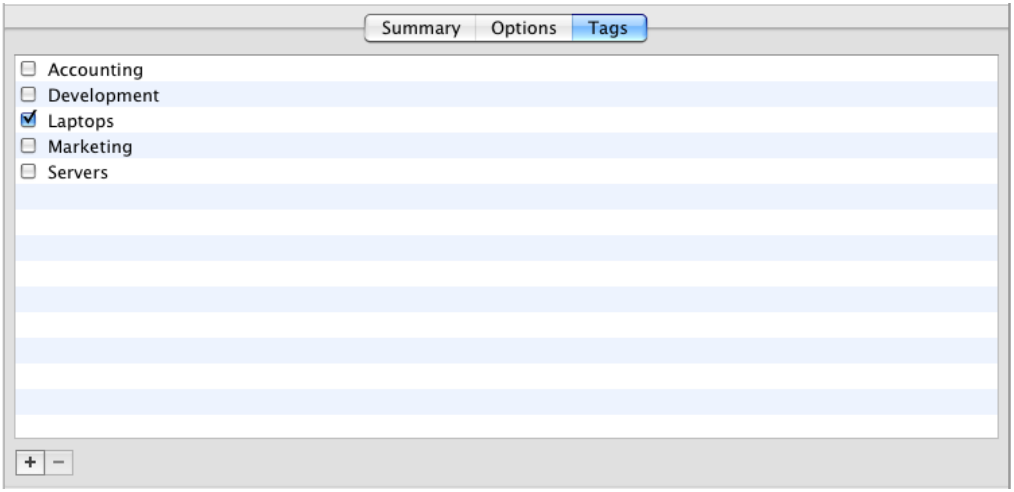
In the Volumes section, from the Back up pop-up menu, you may choose All Volumes, Selected Volumes, or Startup Volume. If you choose Selected Volumes, you must make sure that the volumes that you wish to back up have a checkmark next to them.

Tip: *You can use Selected Volumes to restrict the volumes on a machine that would otherwise be selected for backup by other functions of Retrospect. For example, you could have used a Tag (see below for more on Tags) to select a particular Retrospect Client machine. If you did so, by default all volumes attached to that machine would be backed up. By using Selected Volumes, you can back up just the volumes you want.*

Tags: The Tags tab, empty by default, allows you to create tags that you can apply to particular Sources. These tags can then be used by scripts to perform Retrospect operations only on items with those tags. Tags allow you to group volumes together for better organization. Tags that you create appear in the Scripts category under the Sources tab.

For example, you could make an Accounting tag 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 tag and Retrospect knows you mean all of the volumes within that group. Another possibility would be to create a Laptops tag for all of your portable Retrospect client machines, making it easy to select those machines for inclusion in a Proactive Backup script.

To create a new Tag, click the + (plus) button at the bottom of the Tags tab. After you enter its name in the dialog, the new tag appears in the list.



To assign one or more Tags to a Source, first select the Source in the Sources list, then click the checkboxes next to the Tags that you want. Similarly, to remove a tag from a Source, select the Source from the Sources list, then clear the checkboxes next to the Tags that you want to remove.

To eliminate a tag from Retrospect, select the tag, then click the – (minus) button at the bottom of the Tags tab. Retrospect will ask you to confirm your action. Delete tags with caution; there's no undo if you make a mistake. Deleting a Tag removes the tag from any volumes that you may have applied it to, but doesn't otherwise affect the volumes. You may need to check any scripts that use the tag you deleted.

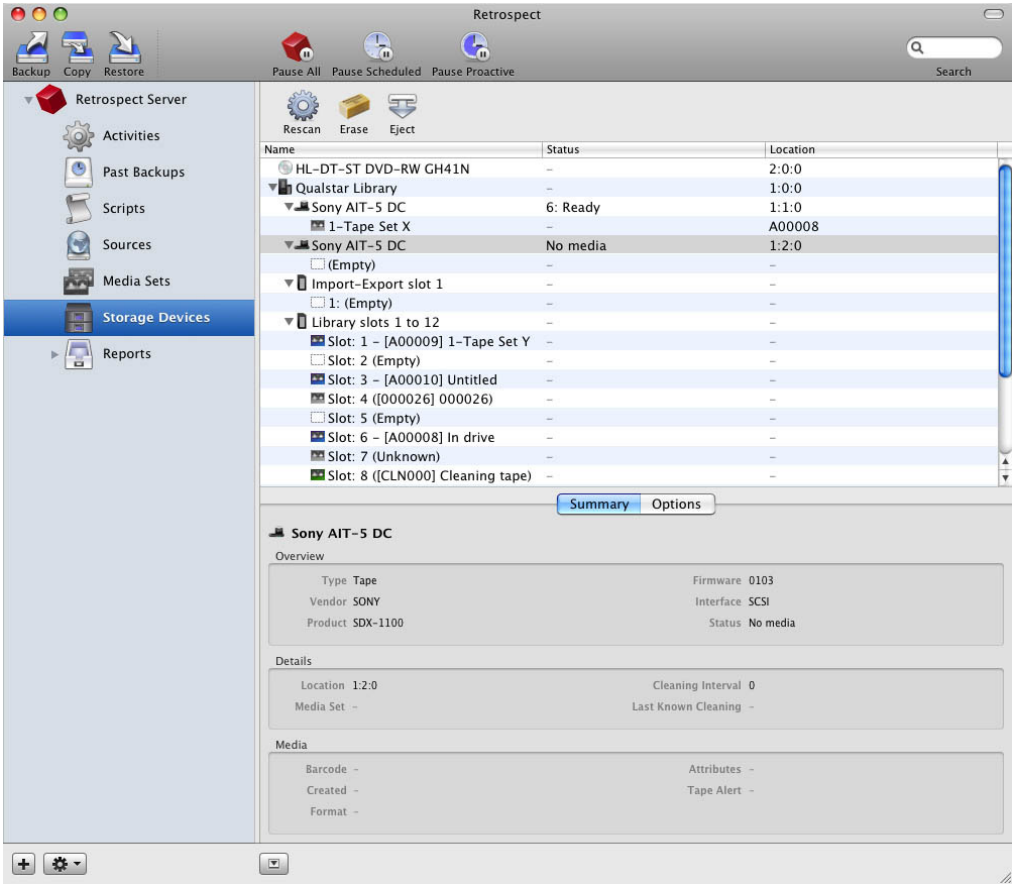
Customizing the Sources List

You can customize the Sources list. You may sort most columns in ascending or descending order by clicking the column header; a selected column is highlighted, and there is a upwards or downwards pointing sort arrow in the column heading. You may change the order of the columns in the list by dragging column headers. Clicking the line between the two columns allows you to drag to change the width of the column.

The default choices in the Sources list are: Status, Name, Machine, Operating System, Space Used, Space Total, Last Backup Date, Capacity, and Browse Files. By right-clicking in any of the column headers, you get a contextual menu from which you may also add additional choices: Path, Interface, Type, Connection, File System, Agent Version, Space Free, and Next Backup Date.

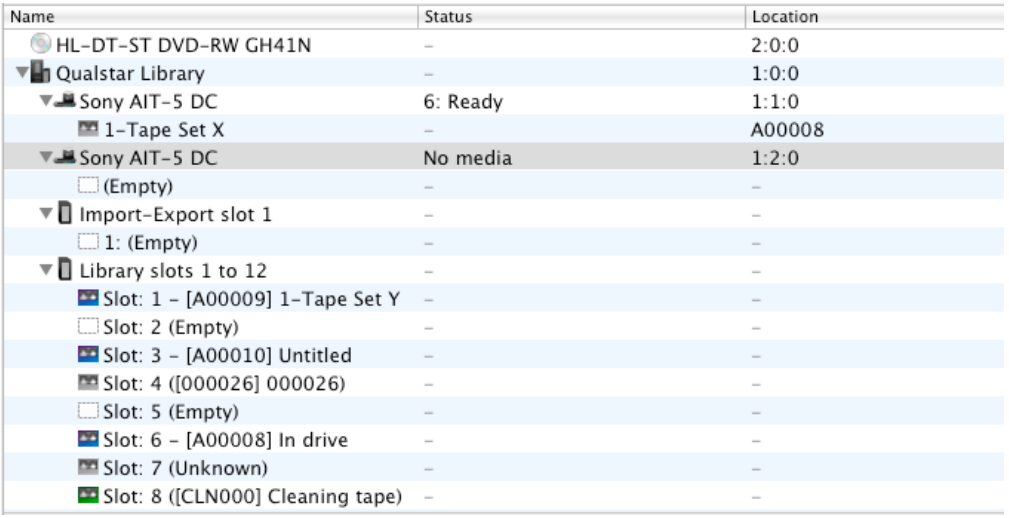
Storage Devices

The other place that your backup hardware may show up in Retrospect is under the Storage Devices category in the sidebar. Devices that show up here are those that are specifically controlled by Retrospect, such as tape drives and libraries (sometimes called a loader, autochanger, or autoloader).



Take a closer look at the Storage Devices list. By default, it consists of three columns: Name, Status, and Location. These work as follows:

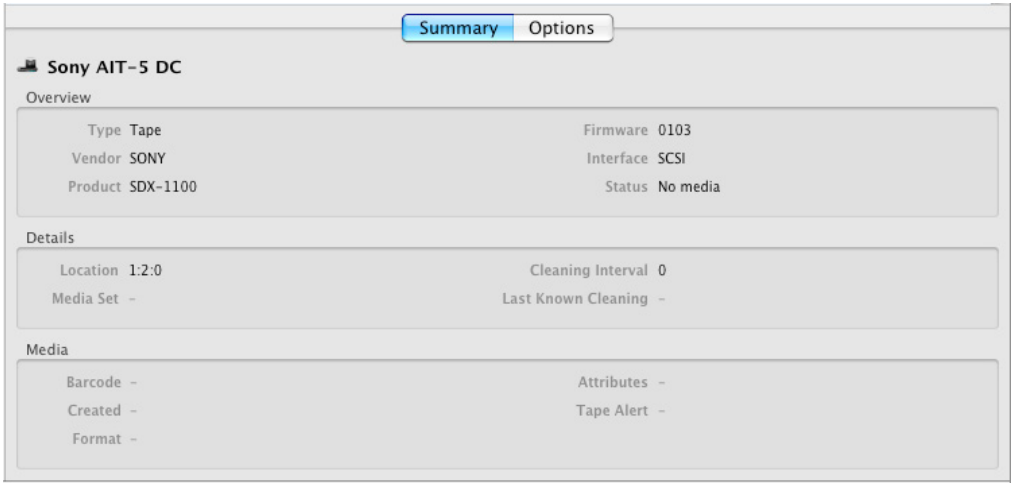
- **Name** displays the name of the storage device, magazine, or media. A gray disclosure triangle will appear to the left of the name for devices that Retrospect can control and use, and it can be toggled to show the media available in that device. If you see a device listed without a gray disclosure triangle next to its top-level name, Retrospect is not able to use that device as a backup destination.
- **Status** shows you the condition of the storage device, as reported by the device. For example, most tape drives will report Ready when there is a tape in the drive that can be written. In the screenshot below, because the device is a tape library, the Device Status for the first drive is 6: Ready, indicating that the tape from slot 6 is in the drive and is ready for use.
- **Location** shows three numbers, broken down into three digits (n:n:n) that represent Bus:ID:LUN. Internal ATAPI (DVD+RW drive), internal SATA, FireWire, USB, and SCSI would each be represented by their own bus. ID is the device's ID on that bus. LUN (which stands for Logical Unit Number) would represent a logical volume's ID on a SAN or in certain iSCSI configurations.



Using the Detail area

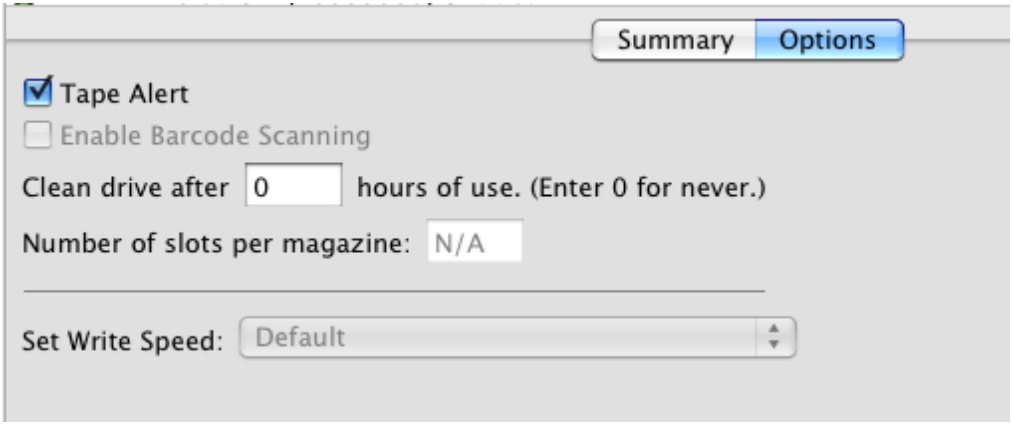
Below the Storage Devices list, the Detail area shows additional information about whichever device is selected in the list. There are two tabs in the Detail area: Summary and Options.

Summary: In the Summary tab, Retrospect shows you information about the selected storage device or media, and that information changes depending on the kind of device or media you have selected.



The Overview section tells you the key information about the device, including its type, vendor, model, firmware version, interface, and reported status. The Details section displays information about the device's location and for tape drives, information about the drive's cleaning interval and last known cleaning. The Media section gives you details about the media in the selected device, including its barcode (used with some tape libraries), when the tape was first used, whether the data on the tape is compressed or not (shown under Format), and other tape attributes.

Options: In the Options tab, Retrospect shows you information about the selected storage device, and the controls in this tab are active or inactive, depending on the kind of device you have selected.



The controls at the top part of the detail area are for tape drives. Checking Tape Alert causes Retrospect to add an alert of the tape drive error to the Log (to see the error, choose View > Log). Some tape libraries can keep track of tapes with a barcode reader; check Enable Barcode Scanning to make Retrospect use barcoded tapes. You can also set Retrospect to alert you to clean your tape drive on a regular schedule by entering the number of hours between cleanings (the default choice of 0 means that Retrospect will never remind you to clean your tape drive). The Number of slots per magazine setting is most useful for libraries with many slots. It lets you group slots together for easier viewing and slot management in the Storage Devices view. Set the maximum number of slots to include in a group and Retrospect will organize the library automatically. 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 an actual physical grouping of slots or magazines; it is for display purposes only.

The Set Write Speed pop up menu is used for optical drives. The default choice will write data to the drive as quickly as the drive can handle it. If you have special needs, such as recordable media that you know cannot handle the fastest speeds, you may choose Fast, Medium, or Slow from the pop-up menu.

Customizing the Storage Devices List

You can customize the Storage Devices list. You may sort most columns in ascending or descending order by clicking the column header; a selected

column is highlighted, and there is a upwards or downwards pointing sort arrow in the column heading. You may change the order of the columns in the list by dragging column headers. Clicking the line between the two columns allows you to drag to change the width of the column.

Besides the default columns listed above, by right-clicking in any of the column headers, you get a contextual menu from which you may also add additional choices to the list: Type, Media Set, Vendor, Product, Firmware, and Interface.

Hardware Overview

To confirm that your backup device is compatible with Retrospect, refer to the Retrospect website for the latest compatibility information and more specific details on supported devices.

If you have problems with Retrospect and your backup devices after you've confirmed you have a valid hardware and software installation, refer to Chapter 8, Troubleshooting and Support Resources.

Working with Retrospect and Your Hardware

Most of the time, your backup hardware will just work with Retrospect. But sometimes you may need to monitor hardware more closely, or troubleshoot problems. This section discusses how to work with specific types of hardware.

Seeing Your Backup Device

To confirm that your backup devices are being seen and can be used by Retrospect, check to make sure that they appear in either the Sources list or the Storage Devices list, depending on the type of device. When you can access a device from the desktop of the Retrospect server, you should also be able to see it in Retrospect, with the exception of network shares, which Retrospect accesses as the root user. For devices that should appear in the Storage Devices list, if you're having problems seeing a device, the first thing you should try is clicking the Rescan button in the toolbar above the Storage Devices list. After you click Rescan, give devices up to two minutes

to appear in the Storage Devices list. All backup devices that are properly connected to the backup computer should also appear in Apple's System Profiler application. If you cannot see the device, refer to its documentation for information on setting up properly.

Troubleshooting Tips:

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.

A drive that does not appear in the Sources or Storage Devices lists may not be supported by Retrospect or may have special requirements. Refer to the Retrospect website `http://www.retrospect.com` for the latest compatibility information and more specific details on supported devices.

Finder-Mountable Drives

Retrospect supports any drive that can be mounted in the Finder as a backup destination (except for optical discs).. This includes internal and external hard drives directly connected to the Retrospect server computer, and hard disks served over the network. Retrospect also supports disk drives with removable media, and solid-state drives (SSD) that mount in the Finder.

To see the volumes available for use with Retrospect, click Sources in the sidebar to display the Sources list.

Choosing the Media Set Type

A mountable disk drive can be the destination for both File Media Sets and Disk Media Sets. There are major differences between these two types of Media Set. Disk Media 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 Media Set as the destination in one operation while, at the same time, be the source for one or more additional operations.

In addition, Disk Media Sets do not have the file size limitations inherent in a File Media Set. A Disk Media Set writes a series of files to the destination media, with each file being no larger than 600 MB (which provides benefits if replicating backup data to other storage).

Note: *Starting in Mac OS X 10.6 "Snow Leopard," Apple changed the way the Finder calculates file sizes, where 1 MB = 1,000 * 1,000 bytes, instead of the traditional 1 MB = 1,024 * 1,024 bytes, resulting in apparent Retrospect Media Set file sizes of 692 MB.*

When saved on hard disks, both File Media Sets and Disk Media Sets can store and access files other than the Media Set data files.

Tip: *If you were a user of previous versions of Retrospect, and used File Backup Sets extensively, make the transition to using Disk Media Sets with Retrospect 8.*

Preparing Mountable Disks for Use

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

To add a disk to a Media Set, see "Adding a Disk to a Media Set" in Chapter 5.

Disk Grooming

By default, when a disk that is a member of a disk Media 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, 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 Media Set Creation Wizard, see "Grooming Options for Disk Media Sets" in Chapter 7.

Warning: Grooming deletes files and folders from the backup media. 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 Media 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 backups not groomed by policy to manually delete from the Media Set.

Grooming is useful as part of a staged backup strategy. See "Staged Backup Strategies" in Chapter 7 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 `http://www.retrospect.com/supporteddevices/`.

Sequential access media is relatively inexpensive, has moderately-large capacity, and has a good sustained data transfer rate. Thus, tapes are well suited for backups, especially in situations where you want to move some of your backups offsite for extra safety, or for long-term archiving.

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 in the Finder when you put it in the drive, so don't expect the tape to appear on your Mac desktop.

Tip: *A staged backup strategy that involves backing up to disk, then copying the backup to tape can help improve overall performance when backing up to tape. This is known as disk-to-disk-to-tape (D2D2T) or disk-to-disk-to-disk (D2D2D) backup, depending on the type of media used. See "Staged Backup Strategies" in Chapter 7.*

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. Don't be surprised if your tapes end up containing 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 may use generous compression rates.

Compression

Compression, which can be done by Retrospect or a capable tape drive, conserves space on your tapes by reducing the size of the data being stored. Compression doesn't actually increase media capacity—a given disk or tape can still 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 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 much faster to let the hardware compress the data than to have Retrospect's software-based routine compress it.*

The amount of compression achieved varies depending on the type of data being backed up. Text files generally compress well, while applications, system files, and already-compressed files, such as audio, video, and PDF files, do not. As a complete generalization, given mixed content on a source volume, compression typically will shrink data to approximately two-thirds 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 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 Activities List.
- Logs the error in the Operations Log.

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

Note: *Retrospect does not automatically enable Tape Alert for most tape drives. You can enable it manually as described under "Storage Devices Options", earlier in this chapter.*

WORM Tape Support

As a result of 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.

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

Warning: *When using WORM tapes, make sure Retrospect's "Automatic skip to blank media" preference is turned off (which is the default setting). You can find this preference by choosing Retrospect > Preferences, then clicking on the Media tab.*

Working with WORM Tapes

Since Retrospect treats WORM tapes differently than normal tapes, it is recommended that you use WORM tapes exclusively with Tape WORM Media Sets.

When you create a new Media Set, you can choose to create a Tape WORM Media Set. See "Creating Media Sets" in Chapter 5.

Tape WORM Media Sets are treated differently than normal tape Media Sets. During an automatic operation (i.e. a scripted operation) that uses a Tape WORM Media 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 Tape WORM Media Set.

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

You can manually add normal tapes to Tape WORM Media Sets and WORM tapes to normal tape Media Sets when Retrospect makes a Media Request during an Activity execution, or by using Retrospect's Add Member to Tape Media Set feature.

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

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 in the Log 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.

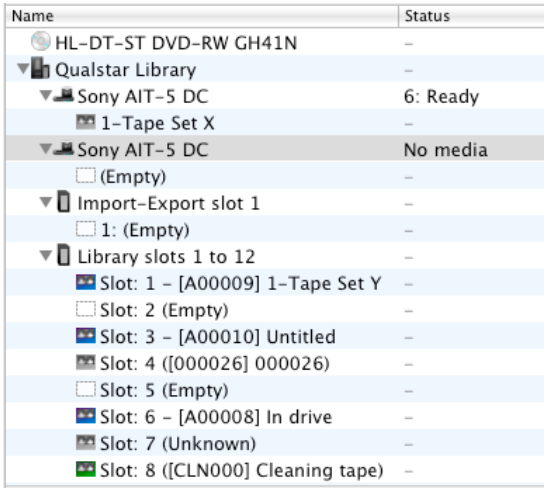
For all tape drives, Retrospect has a option to set the cleaning interval. To access this option, choose Storage Devices in the sidebar, select your tape drive in the list, click the Options tab in the detail area, and enter a number next to "Clean drive after [blank] hours of use." Zero, the default choice, tells Retrospect to never remind you to clean the drive.

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.

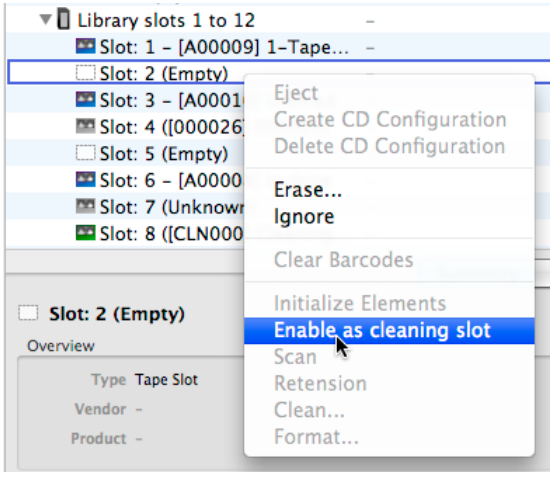
To designate a slot in a library as the cleaning slot:

1. Load the cleaning tape into an empty slot in the library.
2. Click Storage Devices in the sidebar.

3. Select the tape drive in the Storage Devices list. If necessary, click the disclosure triangles to show all the library slots.



4. Right-click on the slot that contains the cleaning tape. From the contextual menu, choose "Enable as cleaning slot."



5. Retrospect changes the name of the tape in the list to "Cleaning tape."

To clean a tape drive manually:

1. If you have a single tape drive, simply insert the cleaning tape. Most tape drives will recognize the cleaning tape, perform the cleaning, and eject the cleaning tape. If you have a tape library, make sure that you have designated a slot as a cleaning slot, as described above.
2. With a tape library, drag the slot that contains the cleaning tape to the drive icon in the list. Retrospect moves the cleaning tape into the drive and the drive automatically performs the cleaning cycle. With some libraries, you can also right-click the tape drive, then choose Clean from the contextual menu. Retrospect asks you to confirm that you want to clean the drive. Click Clean.

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 Device," earlier in this chapter.

To view tape status:

1. Click Storage Devices in the sidebar.

   The Storage Devices list displays.
2. Insert a tape into the drive.

Once a tape is loaded, its status appears in the Status column of the list. The meaning of the status messages are as follows:

- **Ready** indicates the medium contains Retrospect data or is a member of a Media 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 you insert a tape written to by other backup software.

- **Wrong Version** may mean the inserted tape was written to by another version of Retrospect. It can also mean the drive's firmware version is not supported by Retrospect.
- **Write Protected** means the tape is locked.
- **Rewinding** means the tape is in the process of being rewound.
- **Pending** means that the tape is loaded in the drive, but it has not yet been read.
- **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. This message may also appear while a tape is being changed in a tape library.
- **Moving Media** means the tape is being moved from one slot to another, to the tape drive mechanism, or vice versa.
- **Running and Busy** indicate the drive is busy.
- **Empty** 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.

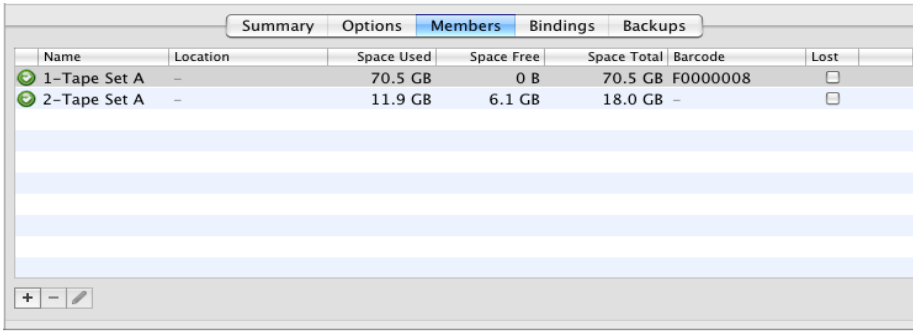
You can also add tapes to a Media Set in advance of Retrospect requesting them.

To add tapes to a Media Set:

1. Make sure that a tape is inserted in your single tape drive, or that there are tapes in the slots in your tape library, then click Media Sets in the sidebar.

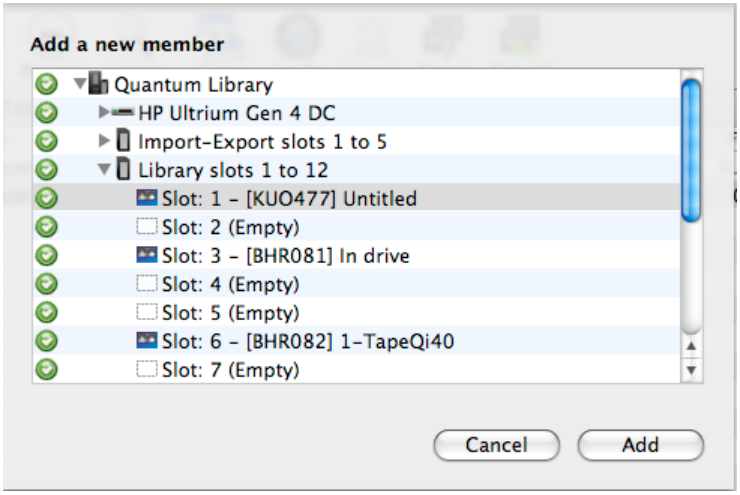
   The Media Sets list displays.
2. Click to select the tape Media Set to which you want to add members.
3. In the detail area below the Media Sets list, click the Members tab.

The Members list displays, showing you the existing members of the Media Set.



4. Click the + (plus) button below the list.

   The Add a new member dialog appears.



5. Select the inserted tape or a tape in a library slot. If necessary, click the disclosure triangles to show all the library slots.

   Note: *You must select blank, erased, or "content unrecognized" tapes. You cannot add tapes that already belong to an existing Media Set.*

6. Click Add.

   Retrospect asks if you're sure you want to add the selected media to the Media Set, and warns that any content on the media will be lost.

7. Click Add.

   Retrospect adds the media to the Media Set, naming the tapes sequentially with the name of the Media Set.

Commands for Single Tape Drives

The following commands for working with tape drives are available by right-clicking the drive in the Storage Devices list and choosing the command from the contextual menu. Other commands in this menu are for use with tape libraries, and are covered under "Commands for Tape Libraries" later in this chapter.

- **Eject** unloads the selected tape from its drive.
- **Erase** erases the contents of the selected tape, and—in the case of some tape drive mechanisms—conditions media to be reused.
- **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.
- **Format** completely reformats the selected tape. This process can be more time-consuming than Erase. It is only supported by certain tape drives.

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 due to unavailable media. 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
`http://www.retrospect.com/supporteddevices/`.

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 list. 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.

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, Media Set properties, Log events, and the Storage Devices list. 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.

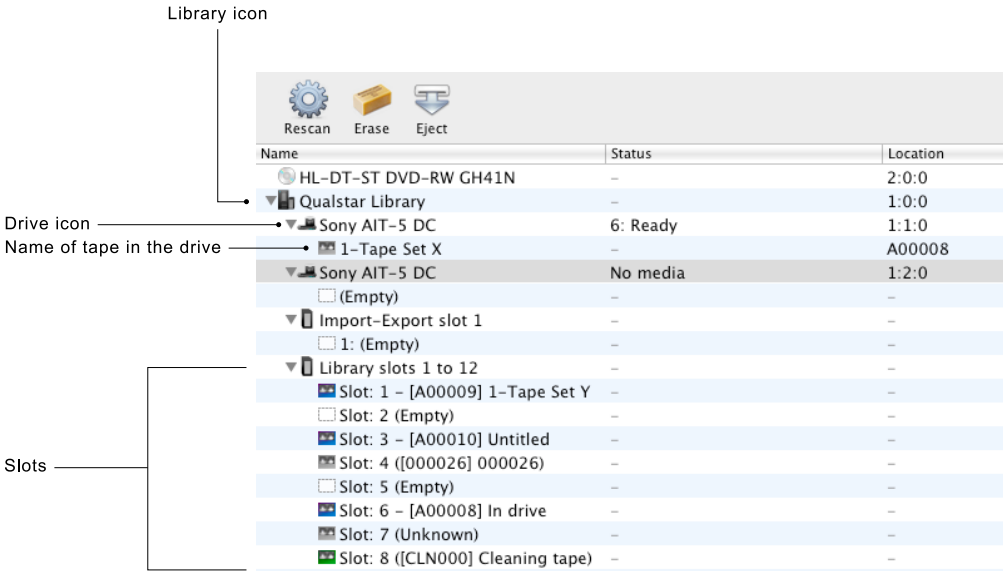
If your library does not support barcode reading, Retrospect must scan the library to get the name of each tape. The library inserts each tape in the tape drive, and Retrospect then keeps track of the tapes' names and locations.

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 in its configuration file.

Viewing Tape Library Status

To view a tape library's status, insert a loaded magazine (if applicable to your device) and click Storage Devices in the sidebar to display the Storage Devices list. Notice how the library, tape slots (including import-export slots), and drive(s) appear in the list.



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.


The slot has no tape.


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.


(Unknown) - The slot has not been scanned by Retrospect.


The slot has been designated as a cleaning tape slot by Retrospect. Cleaning tapes use a green tape icon.

 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.

 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.

 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.

 This tape is formatted as WORM (Write Once, Read Many). See WORM Tape support, earlier in this chapter.

Working with Tape Libraries

In the Storage Devices list, you can move tapes by dragging and dropping their icons. Position the pointer over a tape icon, then you can click and drag a tape from slot to slot, slot to drive, drive to slot, or drive to drive.

Commands for Tape Libraries

The following commands for working with tape libraries are available by right-clicking the library, drive, or slot icons in the Storage Devices list and choosing the command from the contextual menu. Some commands in this menu are for use with all kind of tape devices, and are covered under "Commands for Single Tape Drives" earlier in this chapter.

- **Ignore** tells Retrospect not to scan or use this device.
- **Clear Barcodes** unlinks 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 Retrospect Technical Support.
- **Initialize Elements** sends the Initialize Element 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.

- **Enable as 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.
- **Scan** 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.

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 alert in the Activities list. The operation cannot continue until you insert media.

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.

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. 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-and smoke-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.

How Retrospect Works with Multiple Backup Devices

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. This is useful, for example, to

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 LTO drives.

Retrospect for Macintosh can simultaneously write to multiple devices with the Advanced Tape Support add-on. See the Retrospect website for more information.

Chapter 4: Working with Clients, Servers, and Network Shares

This chapter provides instructions on configuring and administering the Retrospect Client software that allows you to access networked Retrospect client computers from the backup server. It also describes the options and controls available to Retrospect clients. In addition, this chapter explains how to add other networked resources, such as servers and network shares, to Retrospect to be backed up. Finally, you'll find advice about how to best set up your network backups.

Network Backup Overview

Retrospect allows you to use one or more Retrospect server computers with attached storage devices to back up networked Macintosh, Windows, and Linux computers equipped with Retrospect Client software. You can also back up networked servers, such as machines running Mac OS X Server, Windows Server, or NAS devices, in two different ways, which will be explained later in this chapter. If you have more than one Retrospect server, you can conveniently administer them all from a single installation of the Retrospect console application.

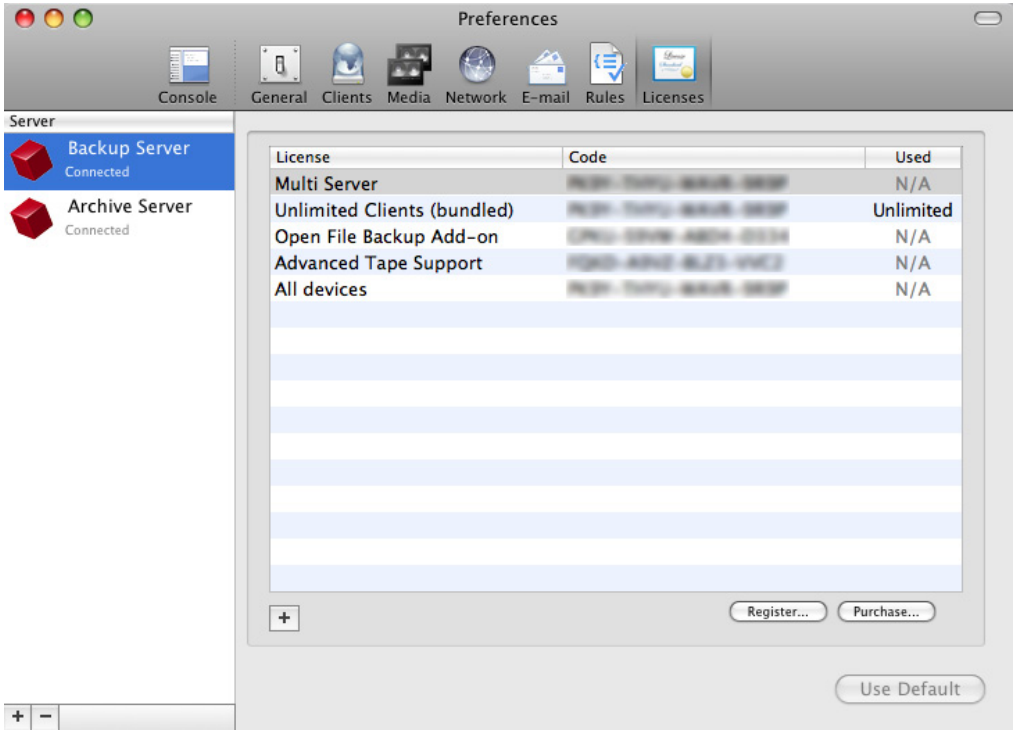
To back up clients, first install the Retrospect Client software on each of the client computers. Then use the Retrospect console application to add those clients as sources for use by the Retrospect server. After configuring the clients, you can create and schedule scripts using client volumes as sources, as if the volumes were connected directly to the Retrospect server.

Client Licenses

Retrospect will work with as many clients as you have licensed. You can add licenses to support more clients.

Retrospect's license manager keeps track of your client licenses with the license codes you enter. Client license codes are included with most Retrospect for Macintosh products and are also available separately in Retrospect Clients Packs.

To view current licenses, choose Retrospect > Preferences, then click on the Licenses tab. If there is more than one server listed in the list on the left, click the server for which you wish to view the licenses. The list on the right shows the different licenses you have added, including client licenses, and under the Used column, shows how many licenses are in use.



Tip: *Licenses are specific to a particular Retrospect server, so if you have more than one server, each server will be running entirely different sets of licenses. For example, if only one of your Retrospect servers has a tape library attached to it, you only need to purchase the Advanced Tape Support license for that server.*

To add a client license, click the Plus (+) button below the license list and enter your new license code in the dialog that appears. To purchase additional client licenses, click the Purchase button below the list.

Working with Retrospect Clients

Installing Retrospect Clients

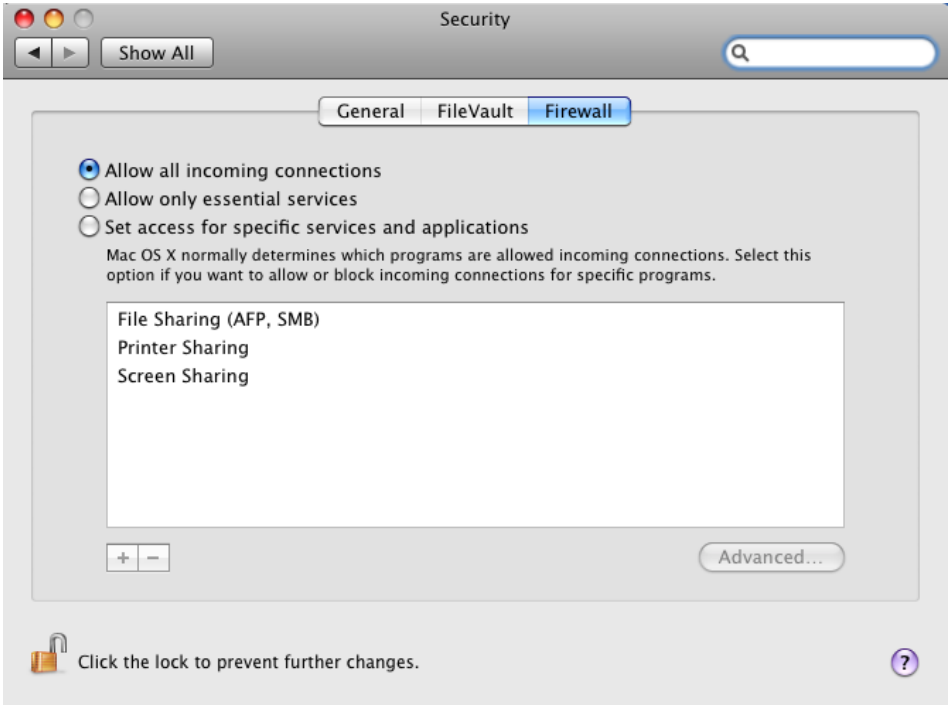
The subject of installing Retrospect Client software on your Macintosh, Windows, or Linux computers is covered in Chapter 1. Please refer to that discussion.

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 UDP 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.

On Macintosh, you control the Mac OS X firewall settings in System Preferences > Security > Firewall.



The default setting for the firewall is "Allow all incoming connections." If you install the Retrospect client with this setting enabled, Retrospect should always be able to communicate with the client.

Warning: *If the firewall is set to the "Allow only essential services" setting when the Retrospect client software is installed, or is changed to the setting after the client is installed and has been added to Retrospect's Sources, Retrospect will not be able to communicate with the client.*

With the "Set access for specific services and applications" setting, the Retrospect Client software installer will work with the firewall to open the required ports so that Retrospect can communicate with the client.

On Windows, if you are using the Windows XP SP2 (or later, including Windows Vista and Windows 7) 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.

Client Security

Retrospect allows you to create highly encrypted private and public key certificate files for your Retrospect Clients. These certificates can then be used to automatically log in clients to the server. This is the recommended method, but you can also enter individual passwords for each Retrospect Client. If you choose to use individual passwords, you will be prompted to enter those passwords when you install the Retrospect Client software.

Using Public/Private Key Authentication with Retrospect Clients

Public/Private Key is a method by which Retrospect Clients running Mac OS X 10.4 or later can be logged into a Retrospect server automatically through use of matching encryption key sets. To use this feature, follow the steps below.

1. Launch the Retrospect application and choose Retrospect > Preferences > Clients.
2. Click "Create keys...", enter a password of eight characters or more for key creation, then click Create. Retrospect may take up to a minute or more to generate the keys, depending on the speed of the computer.

3. If you want Retrospect to automatically log in clients with the proper public key, check “Automatically add clients”. This is recommended. The Retrospect server will then periodically check the network for new clients with the matching public key and automatically add them to Retrospect’s Sources list. Clients so added will be tagged with the “Automatically Added Clients” tag, providing both a place to look in Retrospect for automatically added clients and also a way to create a script that will use the tag to automatically back up such clients. (For more information on tags, see the section on Tags in Chapter 3.)
4. From the Retrospect Installer disk image or CD, open the Client Installers folder, then copy the Mac Client Installer folder onto your hard drive.
5. In the Finder, locate the pubkey.dat file in `/Library/Application Support/Retrospect/` and copy it into the folder named “public_key” inside the Mac Client Installer folder on your hard drive.

6. Distribute or copy this public_key folder containing the pubkey.dat file along with the Retrospect Client installer. As long as the public_key folder is located at the same level with the Client installer when the installer is run, the proper encryption keys (`pubkey.dat, pubkey1.dat, pubkey2.dat,...,pubkey9.dat`) will be installed on each client.
7. After installing the Retrospect Client software on each computer, they can be logged in (or will be automatically logged in, if that option was set) at the Retrospect server.

Network Interfaces

If your backup computer has multiple network interfaces, the Retrospect application and Retrospect Client software automatically switch to the next available network interface if the primary interface is not available.

Mac OS X's Network System Preferences allow you to specify the order in which you want to try different network interfaces when connecting to a network.

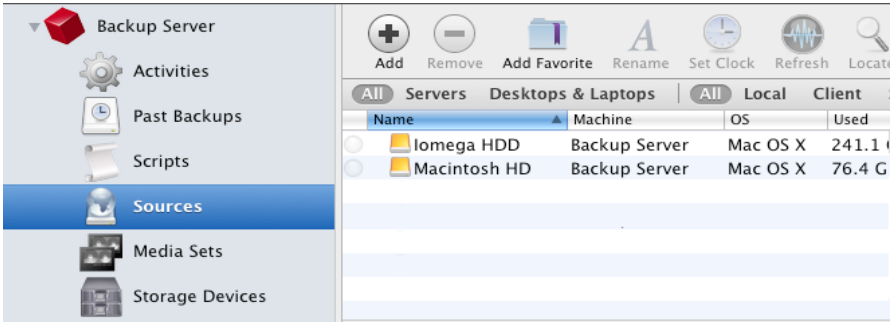
For more information about configuring network interfaces, see "Advanced Networking," later in this chapter.

Adding Retrospect Clients to Sources

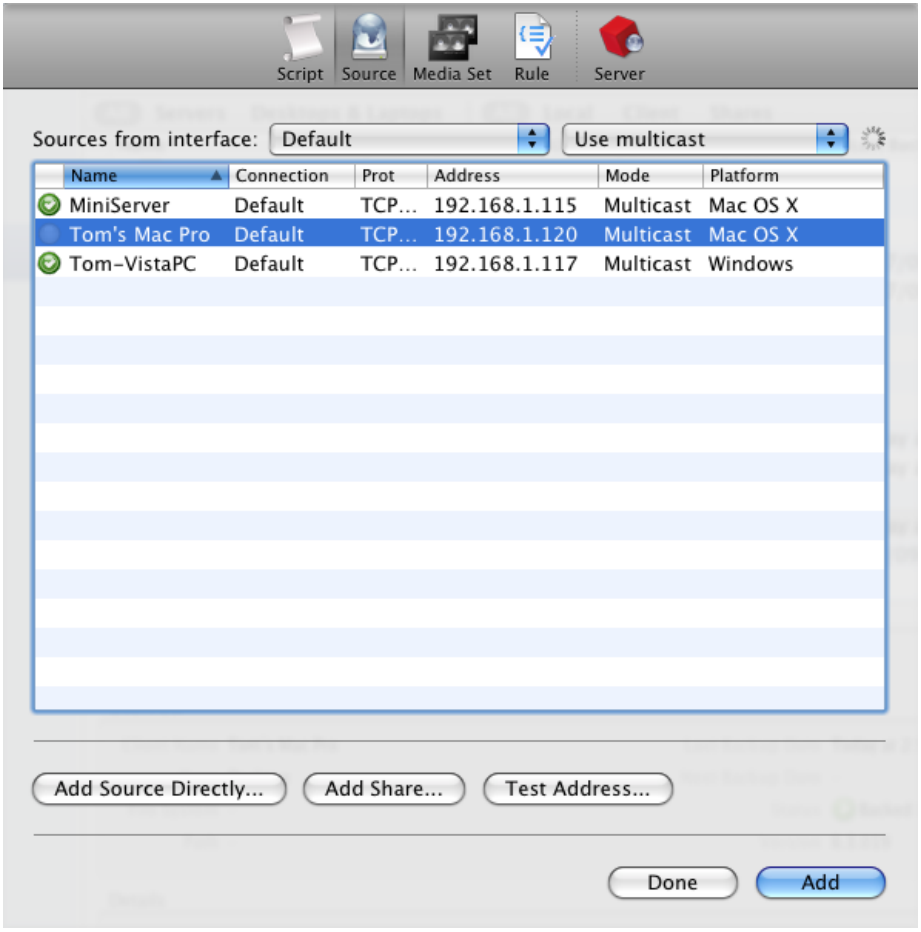
After you have installed the Retrospect Client software on the machines on your network that you want to back up, you must next add those clients to Retrospect's Sources. Clients can be Mac, Windows, or Linux machines.

To add networked clients, follow these steps:

1. In the Retrospect console, click on Sources in the sidebar. If this is the first time you are adding clients, only the local hard disks on the Retrospect server appear in the Sources list. These local hard disks will often be the eventual destinations for your backups.



2. Click the Add button in the List View toolbar. The Source dialog will appear.



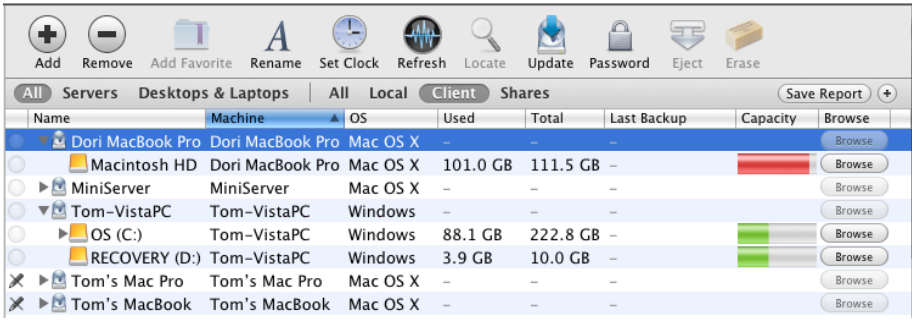
3. If you have more than one network interface, choose the one you wish to use from the “Sources from interface” pop-up menu. Retrospect will search the network for active clients, and they appear in the Source list. If you have set up Retrospect and the Retrospect Client machines to use private/public key authentication, and to add clients automatically, Retrospect will do so without prompting you for a password. Skip to step 6.

4. Click to select a client in the list. If you want to select multiple clients, to which you have assigned the same password, hold down the Command key and click on each client in the list, or click then Shift-click to select a contiguous group.

5. Click Add. If you are not using private/public key authentication, Retrospect will ask you for the password for the client. Enter the password, and click OK. Repeat the process for any remaining clients you wish to add. Retrospect adds the clients to the Sources list, behind the Source dialog. If you have added all the clients you want, click Done to dismiss the Source dialog.

6. (Optional) Sometimes, available clients won't appear automatically in the Source dialog, perhaps because they are outside of the local subnet. You can add these clients manually by clicking the "Add Source Directly" button at the bottom of the Source dialog. Retrospect will display a dialog asking you for the IP address (or DNS or machine name) and password of the client. Enter that information, then click the Add button in the dialog. If Retrospect successfully connects to the client, you will see a green icon, and the client will be added to the Sources list. Click Done to dismiss the "Add Source Directly" dialog, then click Done again to close the Source dialog.

7. Once you are done adding clients, they appear in the Source list, initially as icons with the client machine's names. Click the disclosure triangle next to a machine name to display all of the disk volumes connected to that machine.



Testing Client Connectivity

In order to backup a Retrospect client machine, Retrospect naturally has to maintain a connection between the Retrospect server and the client. Retrospect

provides three ways to test and maintain that connection: Refresh, Locate, and Test Address.

Refresh

First, you can test that a machine with the Retrospect client software that you have previously added to Retrospect's Sources is still reachable using the Refresh function. Follow these steps:

1. In the sidebar, click on Sources.
2. In the Sources list, click to select a Retrospect client machine. To make it easier to find the client machine you are looking for, click the Client button in the Scope Bar, which will make the Sources list only display Retrospect clients. Make sure you click the icon for the machine, not one of that machine's volumes or Favorite Folders.
3. Click Refresh. Retrospect will search for the client machine. If the search is successful, Retrospect will update the information on the client machine in the Summary tab of the Detail view. If the client's volumes have changed, they will also be updated in the Sources list. If the client cannot be found on the network, Retrospect will display a dialog telling you so.

Locate

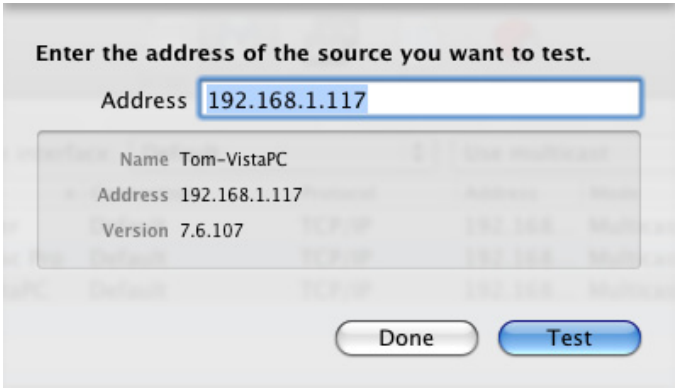
In some unusual situations, Retrospect can have difficulty finding a client. For example, if you add a client using a specific IP address, and that IP address changes, Retrospect may not be able to find the client. In this case, use the Locate feature. Follow these steps:

1. In the sidebar, click on Sources.
2. In the Sources list, click to select the Retrospect client machine you wish to locate.
3. Click Locate. Retrospect will display a dialog similar to the one for adding a client. Locate the client and click Locate.

Test Address

You can test for a responding client at a known IP address, DNS name, or local hostname (found in the Sharing panel of System Preferences, with the name in the format computer name.local). Follow these steps:

1. In the sidebar, click on Sources.
2. Click the Add button in the toolbar. The Add Source dialog appears.
3. Click the Test Address button. In the resulting dialog, enter an IP address, DNS name, or local hostname, and click Test. If Retrospect Client software is found at the specified address, Retrospect reports its client name, address, and client software version. If a computer is found at the specified address, but it is not running Retrospect Client software, or if no computer is found at the address, Retrospect reports an error in the dialog.



Removing a Client

After a client has been logged in, there may come a time when you no longer need it in the Sources list (for example, if the client computer is removed from the network.). In this case, you can tell Retrospect to remove it.

In the Sources list, select the client and choose Remove from the toolbar.

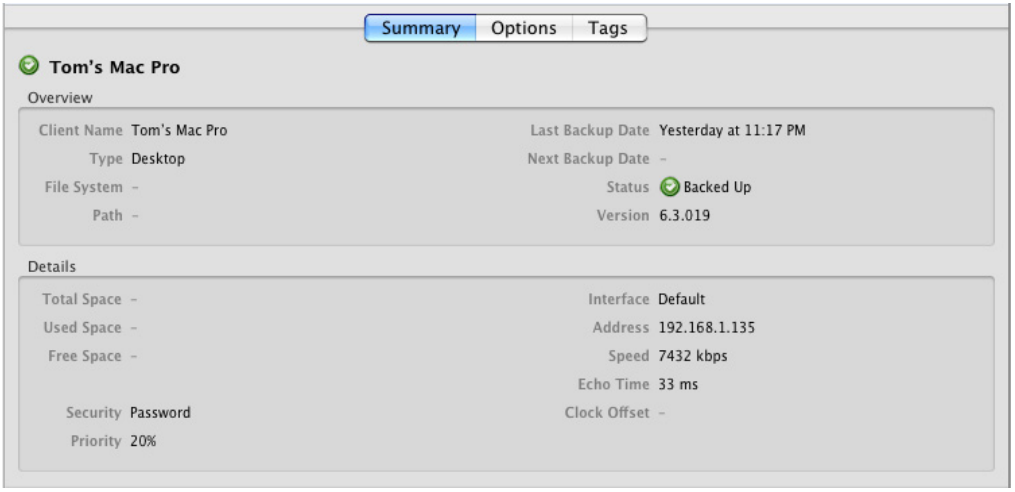
Retrospect asks you to confirm the operation. By clicking OK, you are removing the client volumes from scripts and other lists in Retrospect. This only

affects Retrospect on the Retrospect server in use at the time. It does not affect other copies of the Retrospect server running on other computers on the network, which remain logged in to the client as usual. Removing a client does not affect that client's existing backups.

Removing a client makes one more client license available in the Licenses pane of Retrospect's Preferences.

Getting Information About a Client

In the Retrospect console, you can view status and other information about any client that appears in the Sources list. You'll find that information in the Detail view underneath the Sources list.



The Overview section of the Summary tab view includes the following information:

Client Name is the given client name. This is taken from the client computer, unless you have renamed the client with the Rename button in the Sources toolbar.

Type indicates Desktop or Server.

File System is only active when you have selected a client volume, and lists the file system used by that volume (for example, Mac OS Extended or NTFS).

Path is only active when you selected a client volume or Favorite Folder, and shows the directory path to the selected item.

Last Backup Date shows the last time Retrospect backed up the selected item.

Next Backup Date shows the next time Retrospect is scheduled to backup the selected item.

Status indicates the client's availability for backups and other operations.

Backed Up means the client has been backed up according to a schedule in Retrospect.

Busy means the client is currently being accessed by Retrospect.

Locked means the user at this client workstation has checked the "Read Access 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.)

Offline means the client is not visible to Retrospect, either because it is shut down, off the network, or does not have the client software running.

Ready means the client is a source in a script, but has yet to be backed up by Retrospect.

Unprotected means that Retrospect has never backed up the selected item.

Version is the version number of the client software installed on the client computer.

The Details section of the Summary tab view shows the following information:

Total Space shows the total size of the volume, when you have selected a client volume.

Used Space shows how much space on the volume is in use, when you have selected a client volume.

Free Space shows how much space is available on the volume, when you have selected a client volume.

Security shows the kind of security being used by the client. It will show either None, Password or Public/Private Key. This will also show if the client has the "Encrypt Network Link" option selected (in the Options tab).

Interface is the network interface assigned to the client.

Address is the IP address of the client.

Speed is the transfer rate of the network connection between the backup computer and the client computer.

Echo Time is the time delay, in milliseconds, experienced in communicating with this client, typically under 200ms. If the network or client is busy, or you are using routers, the echo time could easily be higher without indicating a problem.

Clock Offset is the difference in time between the internal clock of the client computer and the Retrospect server.

Updating Clients

As client software is improved, new versions will be made available for download from the Retrospect website. You can then update clients either from the Retrospect server, or from individual clients.

Updating Clients from the Retrospect Server

To update a client from the Retrospect server, follow these steps:

1. In the sidebar, click on Sources.

2. In the Sources list, click to select the Retrospect client machine you wish to update. To update multiple clients, hold down the Command key and click on each client in the list, or click then Shift-click to select a contiguous group.
3. Click the Update 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: Mac OS X, Windows, and Linux. Different client update files may be available from different places such as the Retrospect CD and the Retrospect website `http://www.retrospect.com/supportupdates/updates/`.
4. Select the appropriate client update file, wherever it may be, and click Update. After your confirmation, Retrospect begins updating the client software on the client computers. If you have different types of clients, repeat these steps for each type.

When the update is complete, Retrospect reports the results in the Operations Log.

Updating Clients from the Client Computer

If you do not want to update clients from the Retrospect server as described above, you can update clients directly from the individual client computers. This is done with the Client Installer application (Mac OS X), Setup application (Windows), or rpm or tar installers (Linux), which can also update clients.

Follow the installation instructions (see Chapter 1) appropriate for the computer's operating system. If you are using Public/Private encryption key pairs, remember to include the proper pubkey.dat file in the Retrospect Client installer's public_key folder before running the Client installer.

Uninstalling a Client and Its Software

If you want to remove the client software from a computer, forget the client as described in "Removing a Client," earlier in this chapter. Then see the following sections for each type of client:

- Mac OS X
- Windows
- Linux

Mac OS X

1. Locate your Retrospect 8 disk image or CD and navigate to `/Client Installers/Mac Client/`.
2. Copy the Mac Client Uninstaller to the Macintosh on which you want to uninstall the Retrospect Client software.
3. Open the Mac Client Uninstaller and follow the on-screen instructions to uninstall the Retrospect Client software.

Windows

1. From the Start menu, choose Settings > Control Panel (Windows 2000/XP) or Control Panel (Windows Vista and Windows 7).
2. Double-click Add/Remove Programs (Windows 2000/XP) or Programs and Features (Windows Vista and Windows 7).
3. In the window that appears, select the Retrospect Client software and click Change/Remove (Windows 2000/XP) or Uninstall (Windows Vista and Windows 7).

Linux

The process for uninstalling the Linux client varies depending on how the client software was installed.

For rpm, type the command: `$rpm -e retroclient`.

For tar, manually remove the client software files installed by tar.

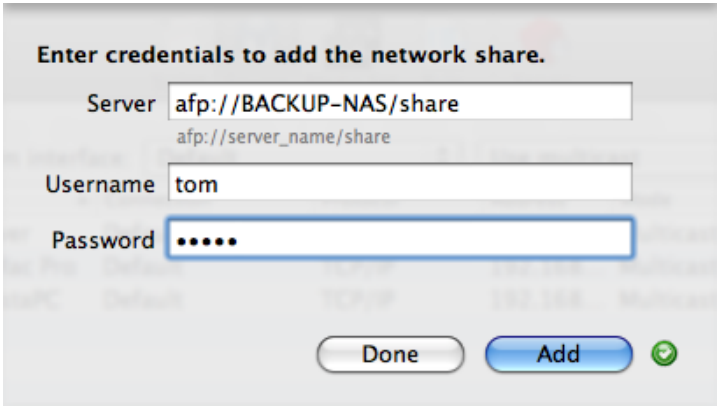
Working with Servers and Network Attached Storage

All versions of Retrospect (with the exception of the Desktop 3-User version) can backup Mac OS X Server or Windows Server machines. And all versions can use Network Attached Storage (NAS) devices as a Source. You add the network share to Retrospect's Sources list by specifying the server's name or IP address, and entering valid login credentials.

Adding a Server or NAS as a Source

To add a network share or NAS to the Sources list, follow these steps:

1. Click on Sources in the sidebar. The local hard disks on the Retrospect server and Clients that you have previously added appear in the Sources list.
2. Click the Add button in the List View toolbar. The Add Source dialog appears.
3. At the bottom of the Source dialog, click "Add Share." A dialog appears asking for the server's credentials. You must enter a URL for the network share, beginning with the abbreviation for the file sharing protocol used by the share. Use `afp://` if the share uses the Apple Filing Protocol; use `smb://` if the share uses the Server Message Block protocol commonly used by Windows computers (Mac OS X machines can also connect to SMB networks). Follow the protocol abbreviation with the name (preferred) or IP address of the share, then a slash, then with the directory name of the shared volume. If the computer to which you're connecting does not have its name assigned by a DNS server, you will need to add the .local domain, such as `afp://serverName.local/shareName`.



4. Enter a username and password for the network share, then click Add. If the information you entered is correct, Retrospect displays a green icon next to the Add button. The network share will also be added to the Sources list behind the dialog. If not, you'll get a red icon, and you should check and renter the information.
5. Click Done to exit the credentials dialog, then click Done again to exit the Source dialog. You'll see that the network share has been added to the Sources list.

Client Preferences

After you have installed the client software, users of client computers can control some aspects of network backup operations with the Retrospect Client control panel. You don't 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:

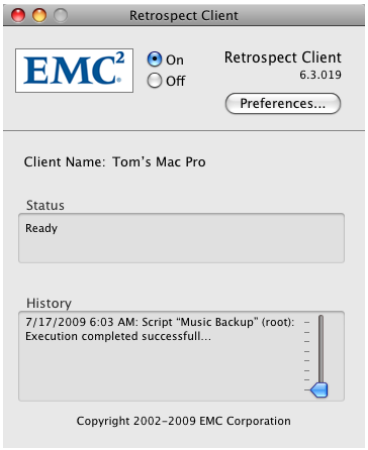
Mac OS X: From the Applications folder, open Retrospect Client.

Windows: From the Start menu, choose All Programs > Retrospect > Retrospect Client.

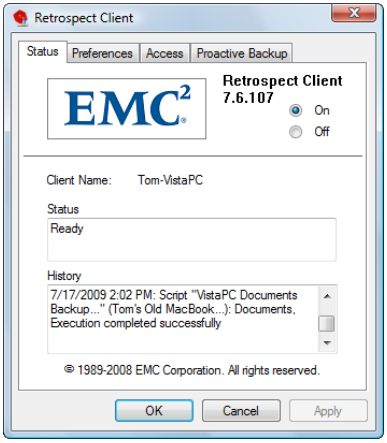
Linux: Run RetroClient.sh from the installed client folder.

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 Mac client looks like this:



Here is the Windows client (the Linux client is similar):



Note: *In addition to the Java-based graphical user interface, Linux clients can also be controlled through the command line. To see the command line arguments, enter the following:* `$retrocpl --help`

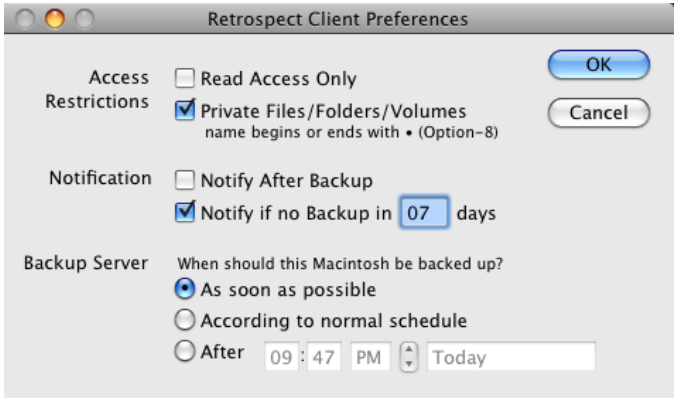
Access Master Control

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.

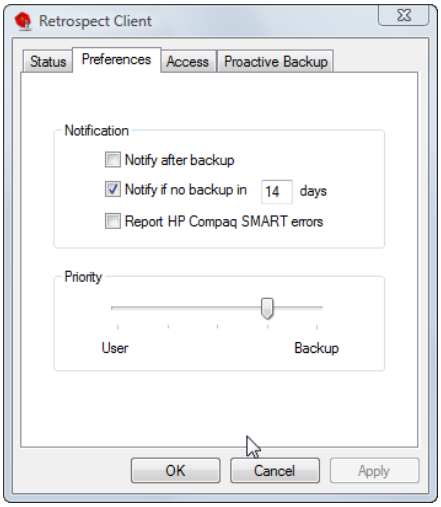
General Preferences

The Retrospect Client control panel has user preferences for managing client operations. Getting to the preferences is done differently under Windows, Linux, and Mac OS X.

Mac OS X: Click the Preferences button.



Windows or Linux: Click the Preferences tab from the four tabs (Status, Preferences. Access, Proactive Backup) at the top of the control panel.



Notification Preferences

These preferences allow client users to specify how they are informed about Retrospect network operations.

Notify after Backup tells the client to display a message after the completion of a backup or other operation. The client's user can click OK to dismiss the message.

Notify if no Backup in *n* days directs the client to display a message after 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 off.

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.

Note: *This preference is not necessary 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. When the slider is set all the way to "Backup," the client operation is given priority and the client computer is less responsive to its user.

This setting only affects the client when it is actively communicating with the Retrospect server.

Access Restrictions Preferences

These preferences allow the client user to control access to the files and folders on his or her computer. On the Mac OS X client, these preferences appear at the top of the Retrospect Client Preferences dialog. On the Windows and Linux clients, these preferences appear on the Access tab.

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 Script options "Set source volume's backup time," "Delete source files after copying and verifying," 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 Linux, 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 X, 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•".

Influencing Proactive Backups

There are two ways to influence Proactive Backup scripts from the client computer:

- Scheduling from a Client
- Deferring Execution

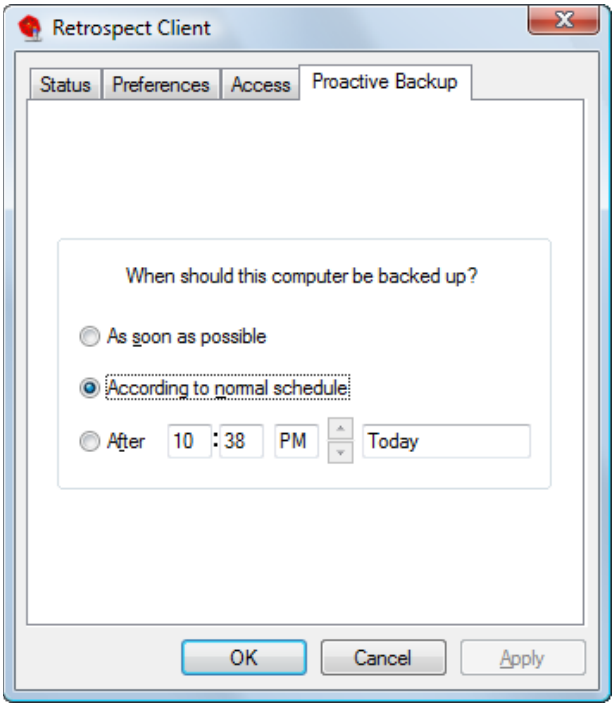
Scheduling from a Client

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 called the Backup Server on the Mac OS X client software.*

Mac OS X: The Backup Server preferences appear in the Retrospect Client preferences window.

Windows/Linux: Click the Proactive Backup tab to reveal its controls.



These controls let the user affect when the client computer can be backed up by the backup computer (using a Proactive Backup script). The user would normally use it to request a backup or defer a backup, but the user can also revert Proactive Backup back to its normal schedule for this client. The Proactive Backup options are:

As soon as possible causes the Retrospect server to back up the client computer as soon as the Proactive Backup is available to do so.

According to normal schedule causes the Retrospect server to 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, with a countdown (set by default to 20 seconds in the Options tab of the Proactive Backup script). 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 Backup to execute.

Clicking **Backup** executes the backup immediately.

Clicking **Defer** lets the user set a later time for the backup to operate.

When a user defers execution, Retrospect makes an entry in the Retrospect server's Log.

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 Add Source 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 Retrospect's Sources 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 Retrospect server. Just exactly how Retrospect gets in touch with the clients depends on the access method Retrospect is using.

The three available methods in the Add Sources dialog are:

- Multicast
- Subnet Broadcast
- Add Source Directly

Multicast

When you first open the Add Sources dialog, the default access method from the pop-up menu is "Use 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. See "Configuring Network Interfaces and Subnets," later in this chapter to learn how to define subnets.

Add Source Directly

You can use the Add Source Directly client access method to add a specific backup client to Retrospect's Sources. 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 directly is most useful for a few clients; adding many will be tedious. One of the other methods would probably be better for adding numerous clients.

To add a client to Sources directly, follow these steps:

1. In the Retrospect console, click on Sources in the sidebar.
2. Click the Add button in the List View toolbar. The Add Sources dialog will appear.
3. At the bottom of the Add Sources dialog, click Add Source Directly. In the resulting dialog, enter the IP address (or DNS or WINS name) and password of the client, then click Add. If Retrospect finds a client at the specified IP address, it displays a green icon in the dialog. Repeat the process for any remaining clients you wish to add directly. Retrospect adds the clients to the Sources list, behind the Source dialog. If you have added all the clients you want, click Done to dismiss the Source dialog.

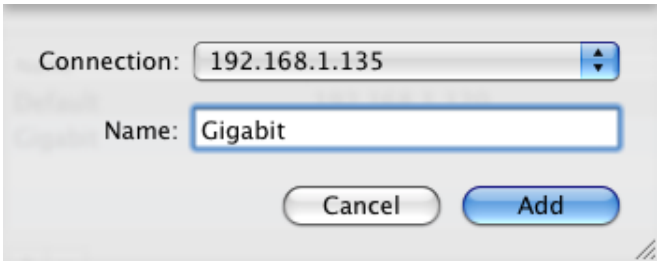
Configuring Network Interfaces and Subnets

Retrospect's interface feature allows you to choose among multiple adapter cards and control networking options for groups of backup clients. For ex-

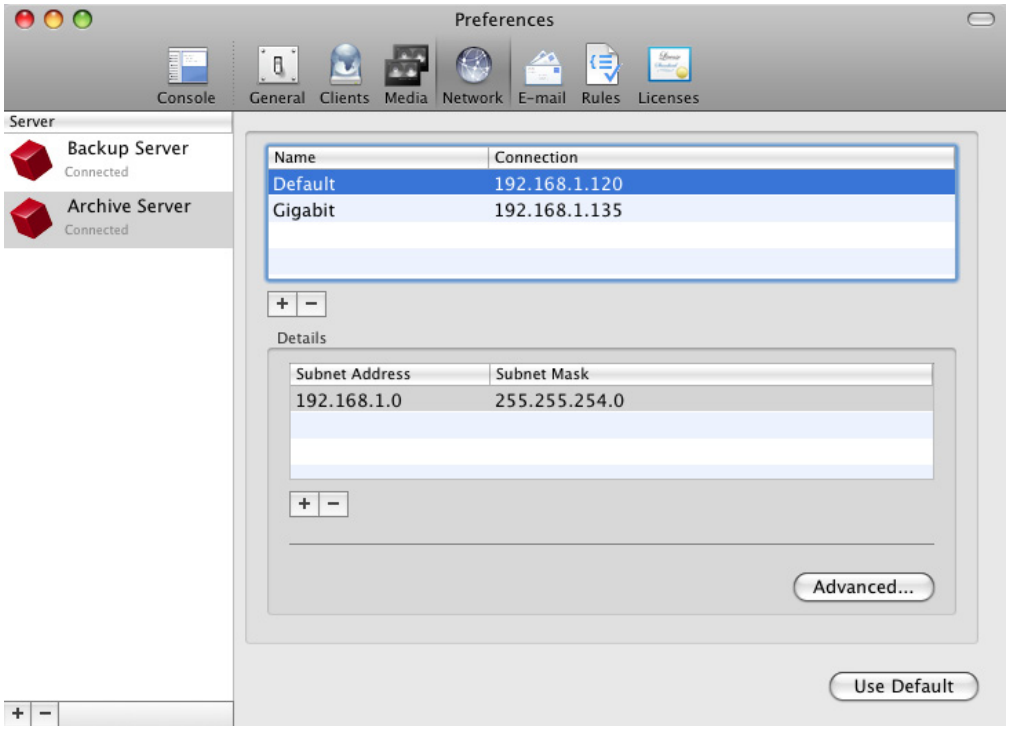
ample, a custom interface lets you back up clients on different subnets without requiring backup data to cross routers, conserving network bandwidth.

You can name and assign different network interfaces to specific network addresses in Retrospect's preferences, which will use the addresses in order. To do this, follow these steps:

1. Choose Retrospect > Preferences > Network. If more than one Retrospect server appears in the Server column, select the server you want to control. In the connection list on the right side of the window, your Mac's default network connect will appear.
2. To add another network interface, click the Plus (+) button below the connection list. In the resulting dialog, choose from the Connection pop-up menu the IP address of the network interface you want to use, then enter a name for the connection and click Add.

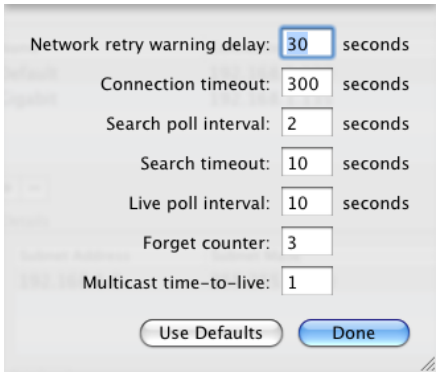


3. The new connection appears in the connection list. You can also restrict the subnet that Retrospect will use when it looks for clients and network shares. To do that, select one of the connections in the connection list, then click the Plus (+) button below the Details box. In the resulting dialog, enter the Subnet Address and Subnet Mask, then click Add. The subnet restriction will appear in the Details box.



Advanced Settings

Expert users may need additional control over Retrospect's network behavior. Clicking the Advanced button in the Network preference pane brings up a dialog with various settings:



Network retry warning delay Retrospect displays its network retry dialog when a client does not respond in the specified time period.

Connection timeout The maximum amount of time that Retrospect will wait for a client to resume communication before logging an error –519 (network communication failed) and continuing to the next activity.

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.

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.

Enter a value next to the settings you want to change, then click Done. If you change your mind after you have entered a setting, click Use Defaults to undo your entries, then click Done.

Warning: *Make changes in this dialog only if you know exactly what you're doing, or at the direction of Retrospect tech support. Under some circumstances, changes in this dialog can adversely affect Retrospect performance. Be careful!*

Network Backup Guidelines

This section provides information and advice to help you set up a workgroup backup using Retrospect.

In general, the same principles that apply to local backups also apply to network backups of client computers. The major difference between a local 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 can't 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 internetwork devices (such as routers or gateways), unless one or more members of the backup workgroup are separated from the rest by an internetwork 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 increase 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. Depending on your capacity and speed needs, one or more high-capacity hard disks, a disk array, a tape library, or a Storage Area Network may be the right backup device for your organization.

Choosing the Retrospect Server

This section offers some advice on how to select the correct computer for the Retrospect server to suit your planned network backups.

You don't need to use a file server as the backup computer. The following table lists various advantages of using a desktop computer or a server as the backup computer.

Advantages of Desktop

- You can use the computer closest to you for easy access to the backup devices.
- 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. This assumes that you don't have a dedicated backup server.

Advantages of Server

- Optimizes your backup speed since server computers are often a high performance model.
- Takes advantage of the server's inactivity during the nights and weekends.
- Gains added security for your Media 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.

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.

Make sure the backup computer has enough RAM to handle the network volume that contains the most files. Retrospect can use more execution threads to get your backups done faster if you add more RAM to the Retrospect server.

If the Retrospect server 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.

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, and because it uses dedicated compression hardware, 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: **Compression**

Description: Allows the backup device to store more files on its media.

Procedure: Finds patterns in the data; the more patterns, the greater the compression.

Implementation: If you have a tape drive that offers compression, Retrospect leaves the task of compression to the hardware since it compresses data faster than Retrospect.

Feature: **Encryption**

Description: Adds security to your backup.

Procedure: Randomizes the appearance of data to prevent unauthorized access.

Implementation: Retrospect always manages encryption.

Feature: **Compression with encryption**

Description: Allows the backup device to store more files on its media and adds security to your backup.

Procedure: Compression must take place before encryption.

Implementation: 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.)

Chapter 5: Working with Retrospect

In this chapter, we'll deal with the heart of using Retrospect, including backing up, archiving, and restoring your data. You'll also learn how to use Retrospect's Proactive Backups to protect data on notebook computers and other occasional visitors to your network. You'll also see how you can monitor Retrospect as it goes about its work.

Each of these Retrospect operations requires creating a script, so you'll learn how to create scripts using Retrospect's Assistants, and also how to create scripts manually. And because you want Retrospect to protect your data without your constant involvement, you'll see how to create and use Retrospect's Schedules to automate data operations.

Preparing for Retrospect Operations

Virtually all Retrospect operations (backup, restore, etc.) require that you create a script that contains the instructions that Retrospect needs to execute the operation. You can create a script manually using the Scripts category in Retrospect's Sidebar, or you can use one of the three Assistants in the toolbar (Backup, Copy, and Restore), which walk you through the process of creating and running a script.

It's possible to add Retrospect Clients, define Sources, and create Media Sets from within the Backup Assistant. But when you are starting with Retrospect 8, it's easier to understand the different parts of the process if you do at least some of the setup before you dive into the Backup Assistant. See Chapter 4 to see how to add Clients and network shares to Retrospect's Sources.

Add Media Sets

Media Sets are the destination for the backups that you make with Retrospect. As discussed in Chapter 2, there are several types of Media Sets. Each Media Set consists of one or more members. For example, each tape in a Tape Media Set is a member of that set. When you add a Media Set to Retrospect, you need to create the set (which for most types of Media Set also specifies where the Catalog for that set will be created and stored) and you also have to specify the location of the first member of that set.

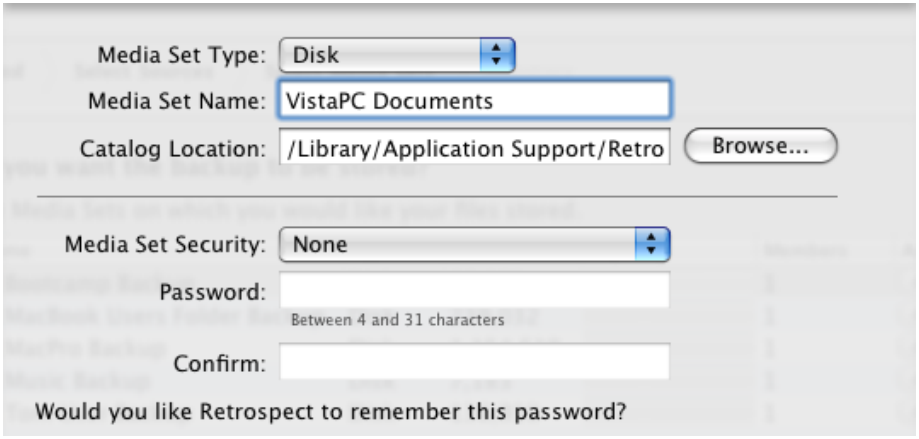
Note: *The Backup Assistant helps you create a Media Set and add its first member, so if you will be using that Assistant, you may prefer to forego creating Media Sets before jumping into your first backup. See "Using the Backup Assistant," later in this chapter.*

To create a Media Set:

1. In the Retrospect console, click on Media Sets in the sidebar. Any Media Sets that you have previously added appear in the Media Sets list.
2. In the List View toolbar, click Add. The Media Set creation dialog appears.

3. From the Media Set Type pop-up menu, choose Tape, Tape WORM, Disk, Optical, or File, depending on the kind of Media Set you want to create. In this example, we'll create the most common Retrospect Media Set type, a Disk set.

4. In the Media Set Name field, enter the name of the set.



5. The Catalog location defaults to `/Library/Application Support/Retrospect/Catalogs/`. Most of the time, the default location does not need to be changed. If you would prefer to change it, click the Choose… button, navigate to the new location from the resulting Browse Files dialog, then click the Select button, which will return you to the Media Set dialog.

6. If desired, make a selection from the Media Set Security pop-up menu. You may choose None, or you may choose to add a password to the Media Set, or choose from four levels of increasingly secure encryption. Any selection other than None requires you to enter and confirm a password for the Media Set.

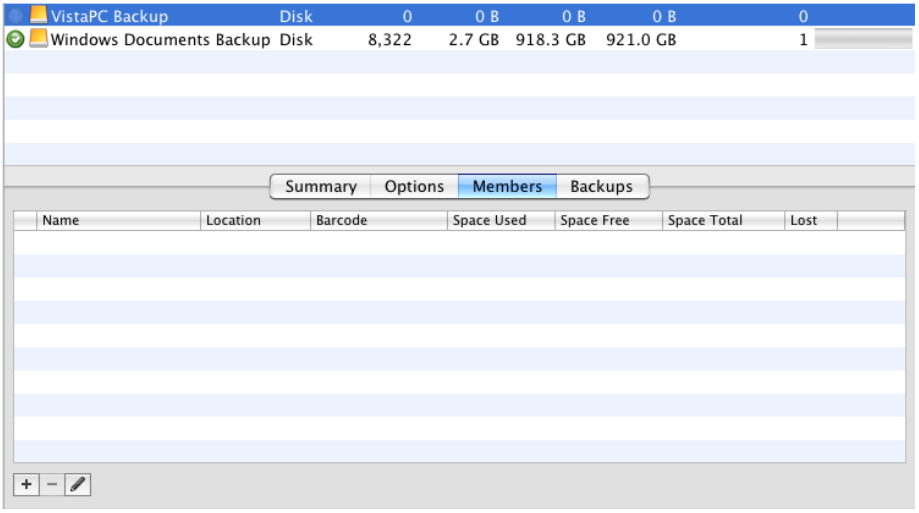
7. If you chose any form of Media Set security, the "Would you like Retrospect to remember this password?" pop-up menu becomes active. The default choice is for Retrospect to remember the password for scripted access, so that you do not have to enter a password every time any script that uses this Media Set runs. You also have the option to have Retrospect never remember the password, or always remember the password for any access to the Media Set.

Warning: *If you set a Media Set password, Retrospect can remember it, but for your security, there is no way to retrieve the password. You must keep track of the password yourself; there is no backdoor password access.*

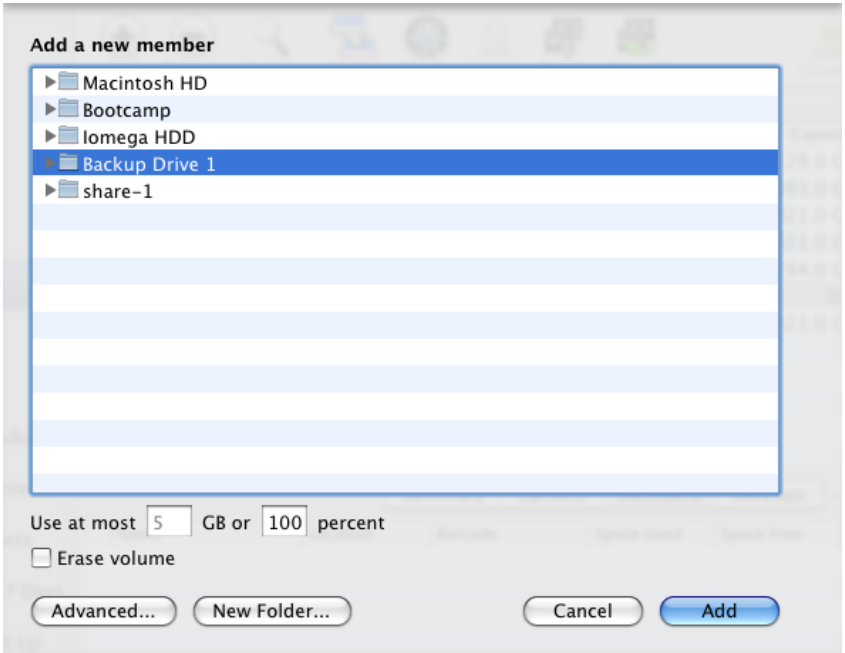
8. Click the Add button to dismiss the Media Set dialog. The new Media Set is added to the Media Set list.

Retrospect will automatically prompt you to add the first member to a Disk Media Set. To add a member to a Tape Media Set (or manually add a member to a Disk Media Set):

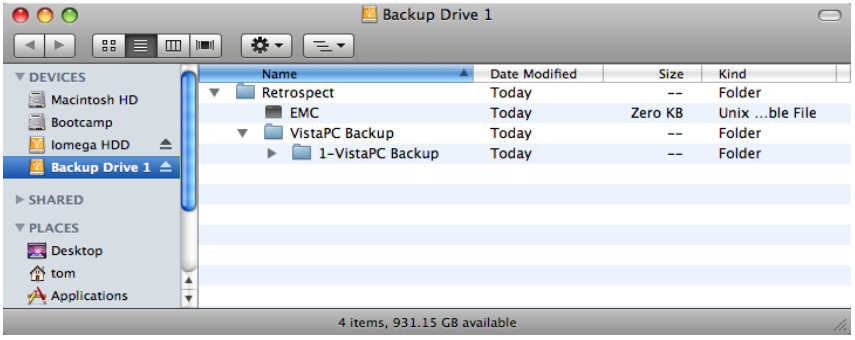
1. Click the new Media Set in the list to select it, then in the detail section of the window, click the Members tab.



2. At the bottom of the Members tab, click the plus button (+). In the resulting "Add a new member" dialog, select where you want the Media Set backup data to be stored. Note that for a Disk Media Set you have the option, at the bottom of the dialog, to specify the maximum size in gigabytes or percentage of the destination hard disk that can be taken up by the Media Set. Click Add.



3. The new member is added to the detail section of the Media Sets list. For Disk Media Sets, Retrospect adds a Retrospect folder on the member disk you have defined, containing another folder with the name of the Media Set, which in turn contains another folder with the Media Set member number. For Disk Media Sets, Retrospect will create a series of 600 MB (or smaller) files inside this folder.



Backing up

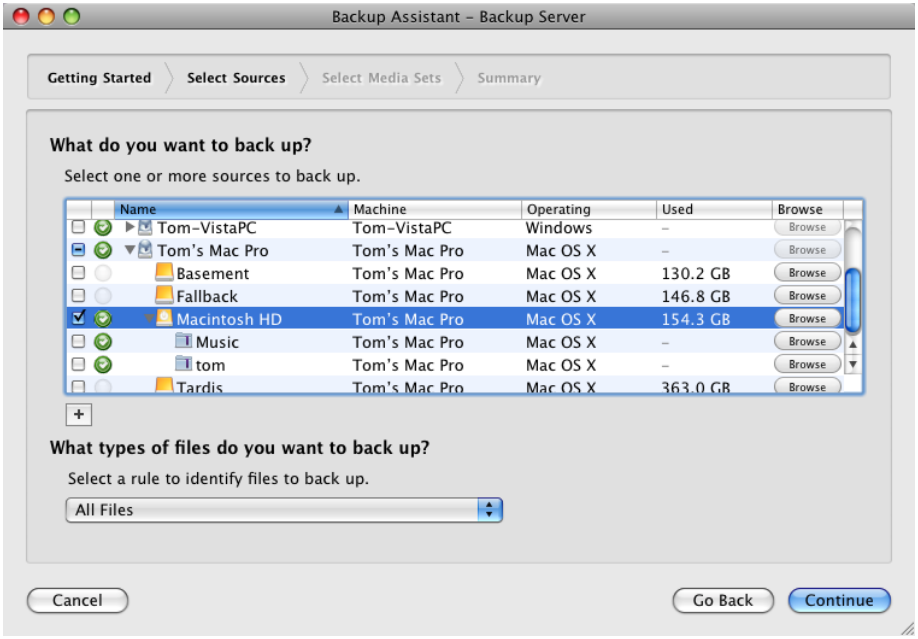
This section describes how to perform backups with Retrospect. The procedures described here include all the information you need to know to effectively back up all of your files.

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

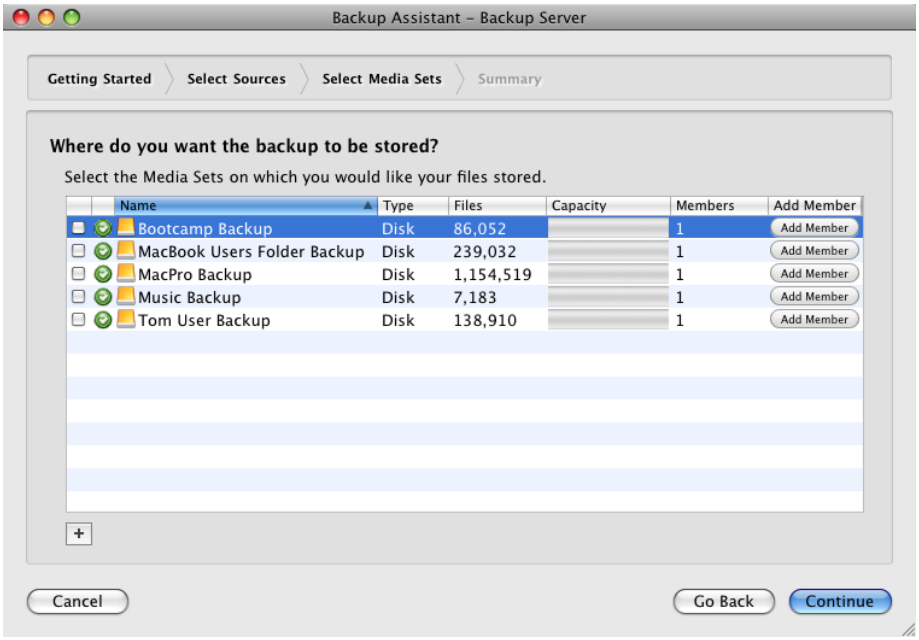
Using the Backup Assistant

To create a backup script with the Backup Assistant, and perform a backup:

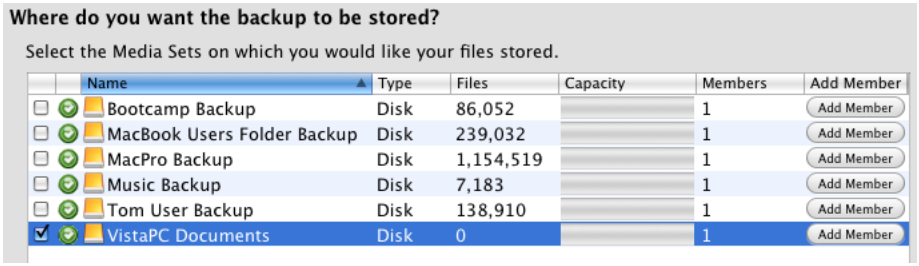
1. Click the Backup button in the Toolbar. The initial Backup Assistant window appears, informing you that you'll be guided through the necessary steps to create a backup. Click the Continue button. The Select Sources pane appears.
2. In this pane, you'll tell Retrospect what it is you want to backup. If you previously established Sources, all of them are available to you in the list. You can select more than one Source to be backed up, and you can choose entire volumes, Favorite Folders, or a combination. Click the checkbox next to one or more Sources.
3. You can specify the kind of files that you want to back up by choosing one of the Rules from the pop-up menu under "What types of files you want to back up?" For example, you can choose to back up All Files (the default), All Files Except Cache Files, or any other saved criteria specified in the Rules section of Retrospect's Preferences. See Chapter 7 for more about Rules.
4. Click Continue. The Select Media Sets pane appears, with a list of Media Sets.



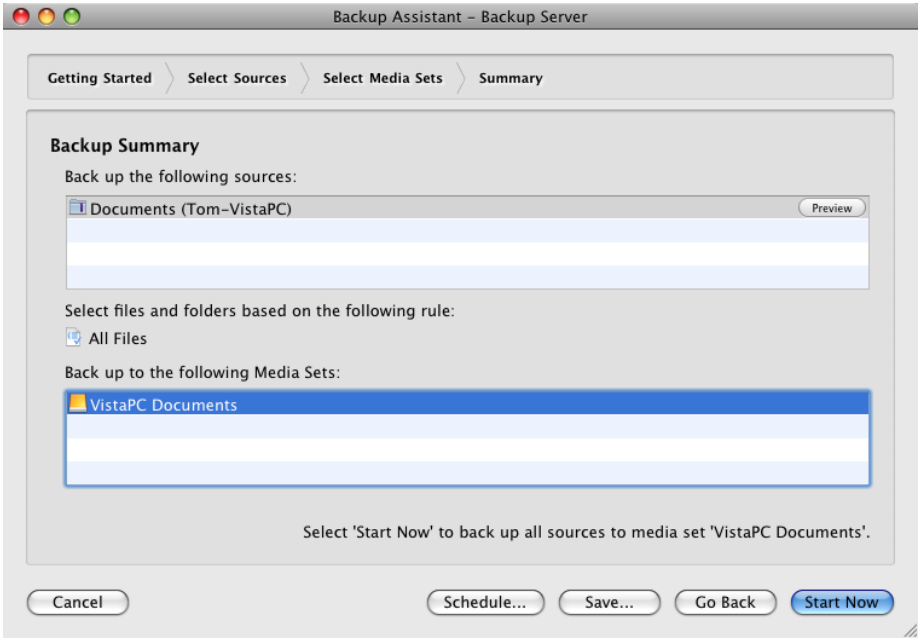
Note: *You can add new clients or Favorite Folders to the Sources list from within the Backup Assistant. To add a new client, click the plus button (+) below the list, then follow the instructions found in Chapter 4 under "Add Clients to Retrospect's Sources." To add a new Favorite Folder, click a source's Browse button in the Backup Assistant, find the folder you want to designate as a Favorite, then click "Add to Favorite Folders."*



5. If you previously created a Media Set as the destination for this back-up, click its checkbox, then click Continue and skip to Step 9. If you haven't yet created the Media Set, click the plus button (+) below the list. The Media Set dialog appears.
6. Choose the Media Set Type from the pop-up menu, and enter a name for the Media Set. You may optionally change the location for the Media Set's Catalog and set security options for the Media Set (for more details on these options, see the instructions found earlier in this chapter under "Add Media Sets"). Click the Add button.
7. Retrospect adds the new Media Set to the list, then (if you chose the Disk Media Set type) displays a browse dialog so you can specify where the first member of the Media Set should be stored. Choose where you want the backed up data to be stored, then click Add.
8. The browse dialog disappears, and you can see that the new Media Set has been added to the list, that it has been selected, and that it has one member. Click Continue.



9. The Summary screen appears, recapping the sources and destination of the backup.



10. (Optional, but recommended) Click the Save button to display a dialog where you can give the script a name. If you do not, Retrospect will name the script "Backup Assistant date and time created," which may make it difficult to later tell at a glance the purpose of the script. Enter the script name, then click Save to return to the Backup Assistant's Summary screen.

11. (Optional) If you would like to set up a schedule for the script to run at a later time, click the Schedule button. The Assistant changes to the

scheduling interface, with a default schedule set. See "Working with Schedules," later in this chapter, for more details on scheduling. When you're done setting up the schedule that you want, click Start Now, which saves the script and its schedule. The script will run automatically at the date and time you specified.

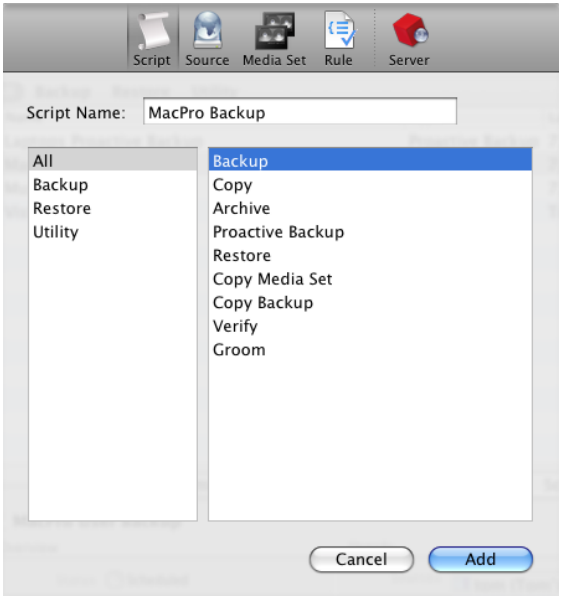
12. If you have skipped the optional steps above and want to immediately run the backup script, click Start Now. Retrospect will still save the script settings as described above.

Creating a Backup Script Manually

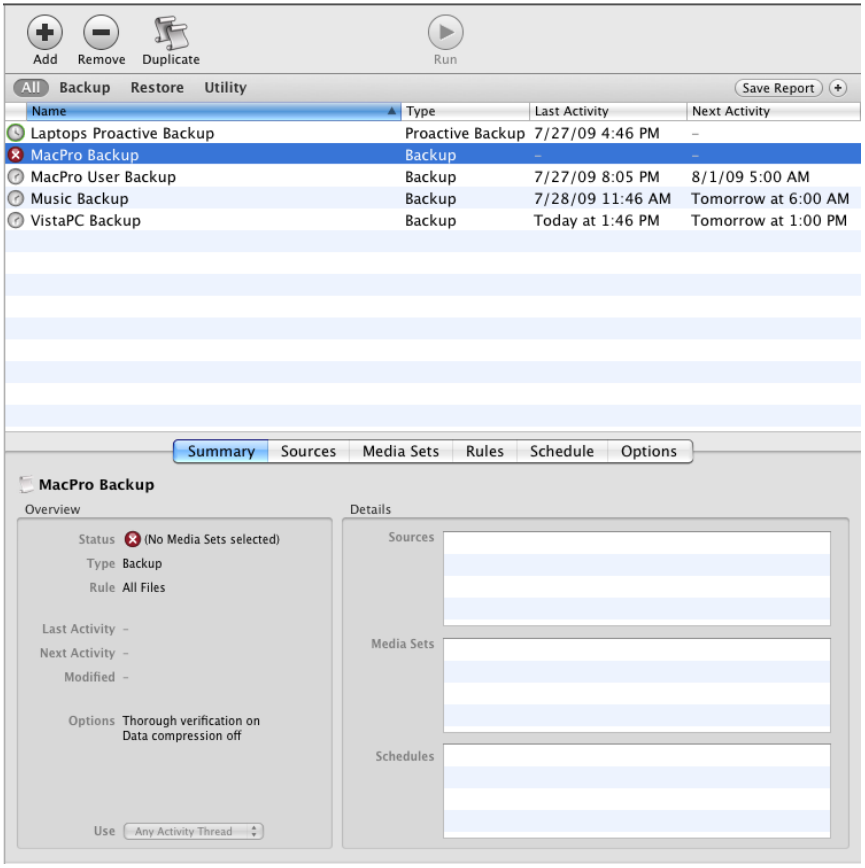
If you don't want to create a backup script using the Backup Assistant, you can create a script manually. This has the added benefit of allowing you to make further adjustments to the script, to customize it for your needs. Of course you can also make these changes to scripts that you create with the Backup Assistant, after the Assistant has done its work.

To create a backup script manually, follow these steps:

1. In the Retrospect console's Sidebar, click Scripts. A list of previously created scripts (if any) appears on the right side of the window.
2. In the List View Toolbar, click the Add button. The Script dialog appears.
3. In the Script Name field, enter a name for your new script.

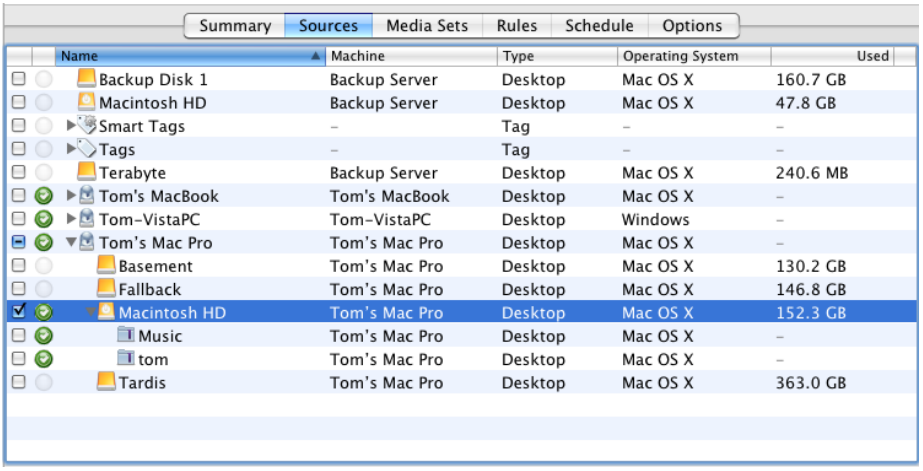


4. Since we are creating a backup script, make sure that the All or Backup category is selected, then click Backup in the script types list on the right side of the dialog, then click Add. The new script appears in the list, with a red icon next to it, indicating that the script is not complete. Below, in the Details area of the Summary tab, you can see that it is blank, telling you that you need to add one or more Sources, Media Sets, and Schedules.

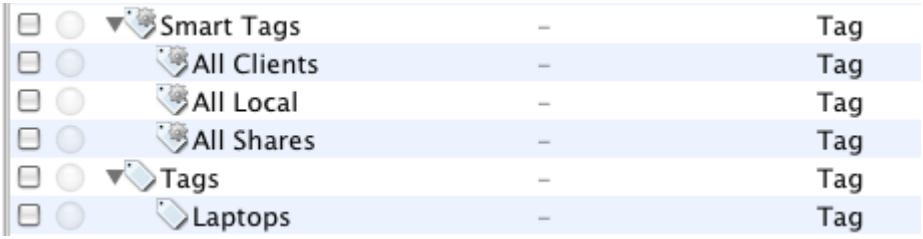


5. Click the Sources tab. Retrospect displays the Sources that you have already defined. Select the Sources that you want to include in the backup by clicking the checkboxes next to them. If necessary, click the disclosure triangles for Retrospect Clients or network shares to see the volumes or Favorite Folders they contain. You can choose Sources local to the Retrospect server, Retrospect Clients, or network shares. Any of these Sources may also have Favorite Folders, which may be backed up independently of the disk on which they reside.

   Note: *If you don't see the source that you need, you must define that source before you can proceed. See Chapters 3 or 4 if you need to know how to add different kinds of sources.*

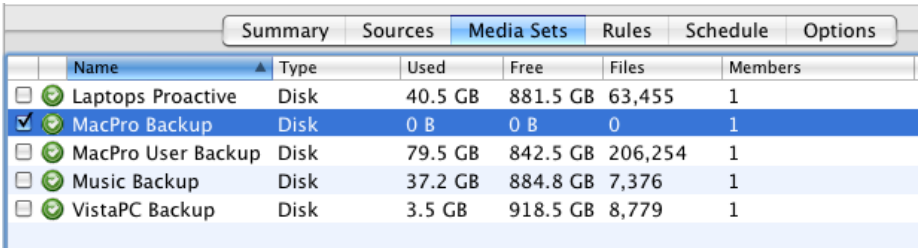


Note: *In the Sources list, you can see two items that need a bit of explanation: Smart Tags, and Tags. These are ways that Retrospect gives you to easily group together and select different Sources. When the script executes, Retrospect will evaluate the Smart Tag or Tag and backup volumes or Favorite Folders that have been assigned to those tags. See Chapter 3 for more information about Tags.*

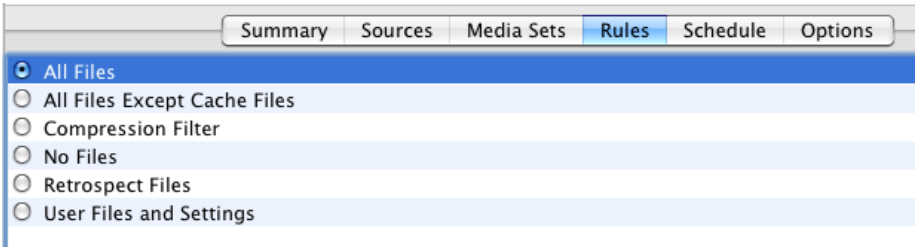


6. Click the Media Sets tab. Retrospect displays the Media Sets that you have already defined. Select the Media Sets that you want as the destination of the backup by clicking the checkboxes next to them.

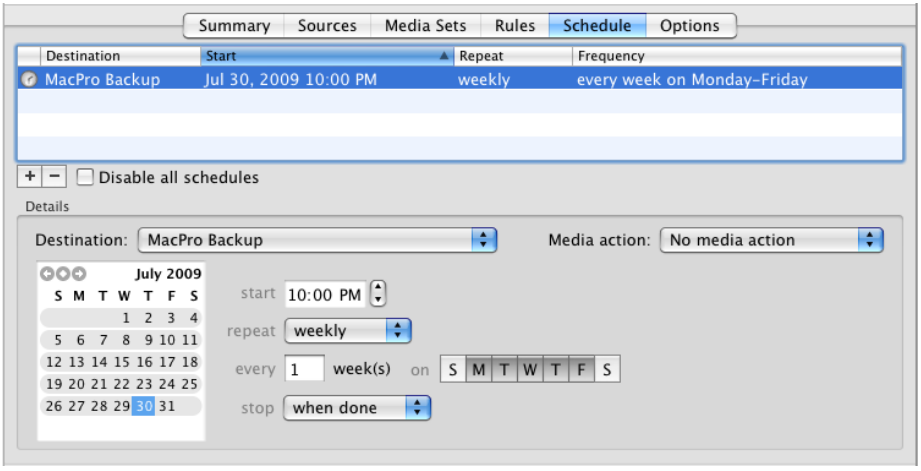
   Note: *You must have defined at least one Media Set before you can proceed. If you need more information, see "Add Media Sets," earlier in this chapter.*



7. Click the Rules tab. Click the radio button next to the Rule that you wish to apply to this backup. The most secure backup is one that includes All Files. For more information about Rules, see Chapter 7.



8. Click the Schedule tab. A script has no default schedule, so you must add one by clicking the plus (+) button under the empty schedule list.

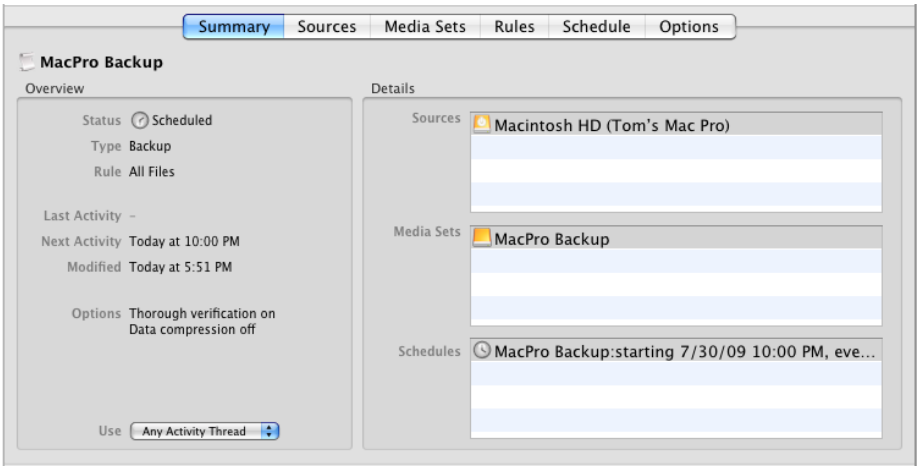


9. In the schedule interface, the Destination pop-up menu lists the Media Sets that you previously selected. If more than one Media Set is associated with this Script, choose the one you want for this schedule from

the pop-up menu. Next, choose the Media action that you want (the choices are No media action, Skip to new member, Start new Media Set, or Recycle Media Set). See Chapter 2 for more information on Media actions. Finally, set the date, time, and frequency for the Schedule to execute. See "Working with Schedules," later in this chapter, for more information.

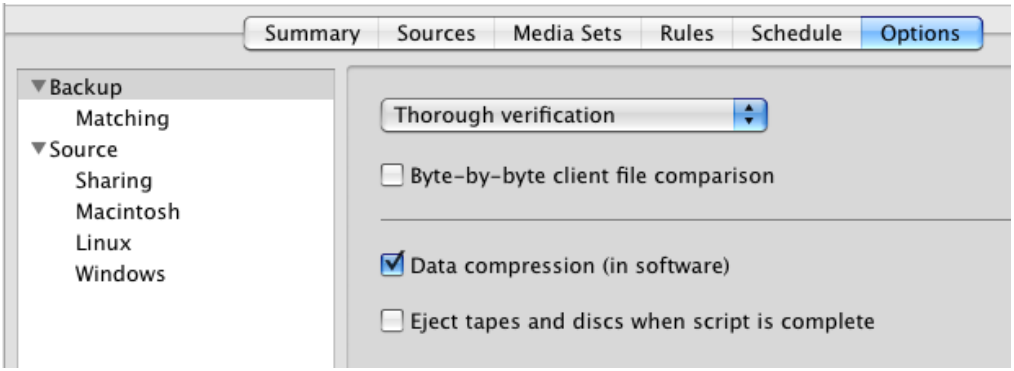
10. Click the Options tab, then set the backup script options you desire. See "Backup Script Options" for more information.

11. Click the Summary tab to review your work. You can now see that Retrospect has all the information it needs to complete the backup.



Backup Script Options

There are many backup options available in the Options tab of the Scripts category. Here is an explanation for each of them. The options are organized into categories, which you can view by clicking the disclosure triangles next to the category name.



The Backup category provides a pop-up menu from which you can choose how Retrospect verifies the backup. The choices in this menu are:

Thorough verification ensures files are copied correctly by comparing files in the destination Media Set with the original source files after the backup is performed. If the backup spans multiple tapes, optical disks, or removable disks, you must reinsert all members to which data has been written. This is a byte by byte verification process.

Media verification compares the files in the destination Media Set to MD5 digests generated during the backup. This method 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 access the original files after the copy phase of the backup. In addition, during backup operations, Retrospect verifies each piece of media as soon as it fills up, so you don't have to reinsert Media Set members for backups that span media.

No verification means that Retrospect will not verify that the backed up files match the original source files. Verification can be scheduled at a later time using a Verification Script.

Other options in the Backup category include:

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.

Data compression (in software): Data compression saves space in the Media Set by compressing files before copying them into the Media 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 Log. The amount of compression savings you can expect depends on the types of files you are compressing. Text files compress substantially; application, media files, and system files do not. Backups using data compression are slower than those without, as are restores.

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.

In the Matching category, there are the following options:

Match source files against the Media Set: This option directs Retrospect to identify previously backed up files during normal backups. This function is a key component of Retrospect's Smart Incremental backups. Retrospect compares the files on the source volume to file information in the Catalog for the destination Media Set.

The Mac OS file matching criteria are name, size, creation date and time, and modify date and time.

The Windows file matching criteria are name and time, size, creation date and time, and modify date. Creation date and time are ignored when they're more recent than the modification date and time.

The Linux file matching criteria are name, size, modify date and time, and creation date and time

Retrospect considers a file already backed up if all of these criteria match.

Note: *Archive script operations have the matching option off by default, which results in archiving all selected files, regardless of whether they are already in the Media Set. Unless you turn on the Move files option, matching is the only difference between archive and backup scripts.*

Don't add duplicate files to the Media Set: This is the other key component of Retrospect's Smart Incremental backups. This option works with the "Match source files against the Media Set" option to prevent identical files previously backed up from being added to the Media Set again. Select both of these options when you want to perform a Smart Incremental backup; that is, you only want new or modified files copied to the Media Set. If this option is deselected, Retrospect adds all files, including previously backed up files, to the Media Set every time a Normal Backup is performed. By default, this option is on and you should keep it that way unless you have a specific need to change it.

Match only file in same location/path: This option 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 files against the Media Set"). When this option is selected, Retrospect uses the unique (and hidden) Mac OS file identification number as an additional part of the matching criteria. This causes separate copies of otherwise-identical files to not match. (And unmatched files get backed up, so your backups become larger and take longer.)

By default, this option is off and you should keep it that way unless you have a specific need to change it.

The Source category has the following options:

Synchronize clock: This option sets the date and time on each Retrospect client computer to match the clock on the Retrospect server. 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.

Speed threshold: This option is useful for preventing backups from becoming too slow. The number you enter here determines the minimum acceptable rate at which the client computer can be 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 skip the client and log an error.

This option is useful, for example, for preventing Proactive Backup scripts from trying to back up a notebook computer volume when it's connected to the network via Wi-Fi or a remote VPN connection.

Retrospect checks the client connection speed only once, as an operation starts. If the speed threshold number is set to zero, which is the default, Retrospect does not evaluate speed and won't prevent an execution for lack of performance.

Activity performance threshold: This option 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 won't halt an execution for lack of performance.

The Sharing category has the following option:

Lock out volumes during backup: This option disconnects users connected to the Retrospect server over the network 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. You can also specify how many minutes advanced warning users will be given. This option will lock out users only for the Retrospect server itself; it does not apply to clients.

The Macintosh category has the following options:

Use attribute modification date when matching: This option is available for backup, archive, copy, and restore operations. By default, it is enabled for all operations except Archive (which does not match files at all unless you choose to do so). When this option is enabled, Retrospect uses the attribute modification date to identify and copy files for which only the extended attributes or ACLs are different. 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 changes 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.

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 copy 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 create Rules 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 default, the volume option is on and files and folders options are off.

Don't backup FileVault sparse image files: Mac OS X since version 10.3 has included a feature called FileVault. When FileVault is enabled, the entire contents of your Home folder is encrypted and decrypted into a sparse image file (in Mac OS X 10.3 and 10.4) or sparse bundle (in Mac OS X 10.5 and later) on the fly. This option tells Retrospect not to back up FileVault sparse images. There are a number of good reasons for this.

The sparse image files change constantly and therefore will always get backed up by Retrospect. In addition, these files can get quite large, and they cannot be restored properly unless they were backed up while the FileVault user was logged out of Mac OS X.

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 Home directory volumes as backup sources.

If a local or client computer has multiple accounts for users that have FileVault enabled, all those users must be logged in.

When they are logged in, their user folders appear in Retrospect's Sources list as separate volumes. For example, if the FileVault user Chester is logged in, a new volume named "Chester" is listed in Retrospect's Volume Selection window.

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.

The Linux category contains the following option:

Use status modified date when matching: This option is enabled by default for backup, copy, and restore entire volume operations. 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 identify 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 different (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.*

The Windows category contains the following options:

Back up System State: This option provides the ability to copy the Windows registry, COM+, active directory, and certificate services when the Windows folder is included in the file selection criteria.

This option is on by default for backup, copy, and archive operations. It is also on by default when you are restoring an entire volume.

In order to restore the System State, the source backup must contain a backed up System State and the destination must be a system volume.

Back up open files: This option allows Retrospect to copy busy files from Windows computers which could otherwise not be copied. It is on by default and requires a license for the Open File Backup option be present.

Protect Multi-Volume Datasets: Building upon the "Back up open files" option, this option ensures that the same point-in-time backup occurs for all volumes attached to the source Windows client. Users without databases spread across multiple volumes may want to disable this option.

Stop when open files cannot be backed up: This option causes Retrospect to halt the operation if the retry timeout occurs or if the Windows client's system

configuration does not support Open File backup. When this option is off, Retrospect backs up or copies all other files (i.e., files that are not open).

Disk inactivity threshold: This option 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.

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 file and 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 and the file's security information, even if nothing else about the file has changed.

Retrospect will keep track of archive attribute changes across Media Sets. For example, if Media Set A includes a copy of a file with new security information and Media Set B does not, the file (and its security information) will get copied during the next backup to Media 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. 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 back up files with new security information.

Back up folder security information from servers: This option 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. When this option is enabled, Retrospect copies folder security information for all the folders on the source.

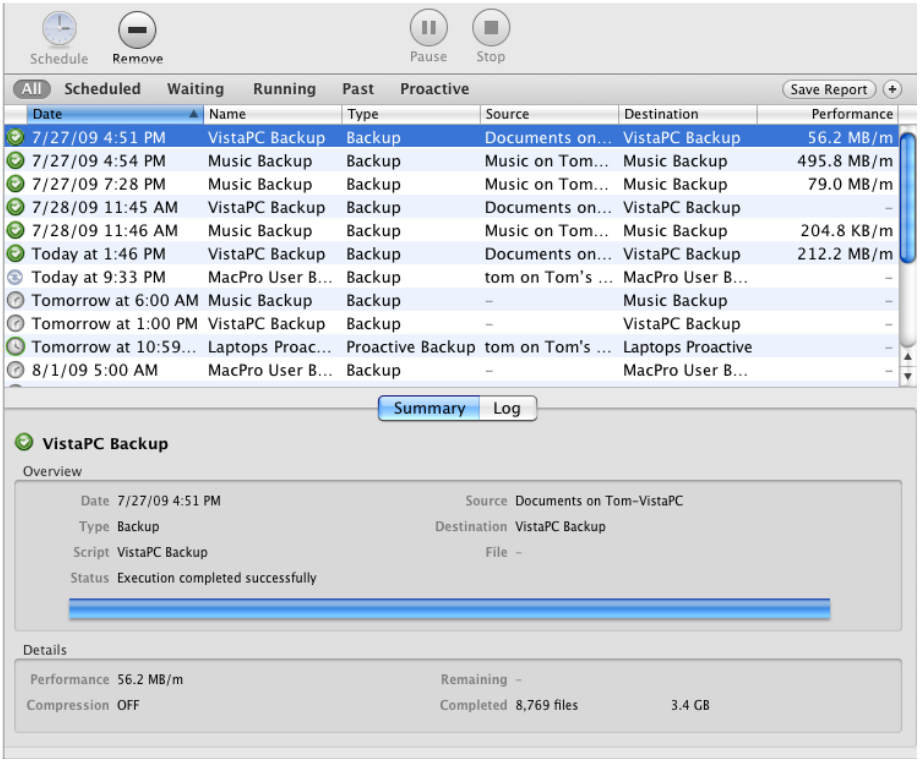
Working with Activities

Retrospect's Activities are where you monitor what the program has done, what it is doing now, and what it will be doing. The Activities list shows you an overview of each time Retrospect runs an operation, and can also show you a detailed log of the operation.

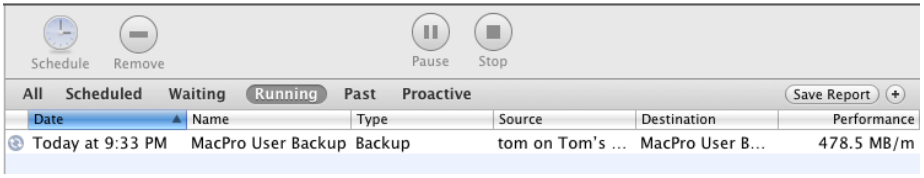
Viewing Running Scripts

One of the things you will probably want to do often is monitor Retrospect's progress during an operation, especially if it is the first time you are running the script that controls the operation. To do this, follow these steps:

1. Click Activities in the sidebar. Retrospect displays the Activity List, showing you past, running, waiting, and scheduled activities.



2. To show just the currently running operations, click Running in the Scope Bar. Retrospect filters the list to show just the operations that are happening now.



Note: *Retrospect lets you know that there is a running operation without needing to show the Activity List; it also shows a spinning progress icon next to the Activities item in the sidebar.*

Controlling Running Activities

When an activity is running, you have the option to either pause or stop it. To do this, click to select the currently running activity in the Activity List, then click either the Pause or Stop buttons in the toolbar. When you click the Pause button, the script execution halts temporarily, the button changes to Run, and a flashing Pause icon appears next to the activity in the list. Click the Run button to resume execution. Clicking the Stop button terminates the selected activity.

Working with the Activity List

You can also use the Activity List to see other kinds of activities besides any currently running activities. You can also see details of a particular past, current, or future activity.

Filtering the Activity List

You can use the Scope Bar to see all the activities, or just specific ones. Click Scheduled to show only future activities (up to the number of activities set in Preferences > Console). Click Waiting to see activities that are waiting for an available activity thread. Click Past to see previously completed activities. And click Proactive to show only Proactive Backups that are scheduled to occur.

Activity List Icons

The leftmost column in the Activity List is the Status column, where Retrospect shows you icons indicating the status of that particular activity. The icons are as follows:

The green icon with checkmark indicates successful execution of the activity.

The red icon with an X in the middle indicates that there were errors during execution.

The clock icon indicates an activity that is scheduled to occur.

The yellow warning icon indicates that warnings were reported during the execution or that the backup was interrupted during execution.

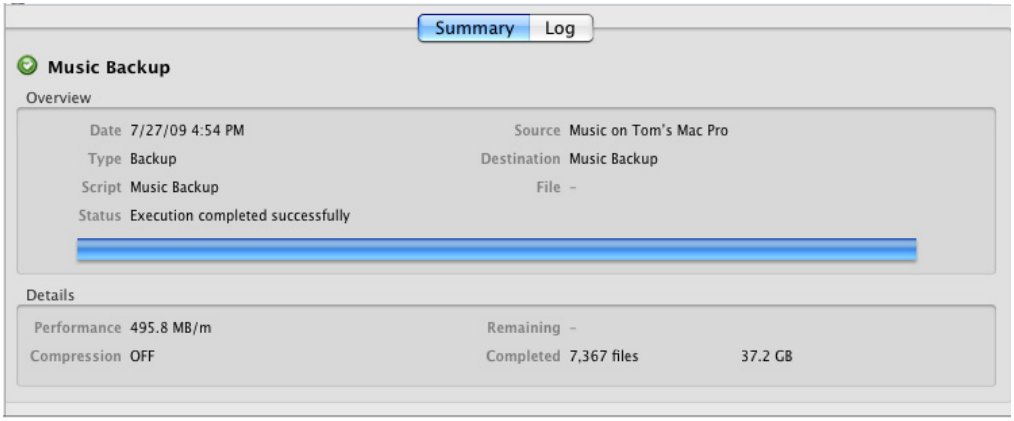
Customizing the Activity List

You can customize the Activity List. You may sort most columns in ascending or descending order by clicking the column header; a selected column is highlighted, and there is a upwards or downwards pointing sort arrow in the column heading. You may change the order of the columns in the list by dragging column headers. Clicking the line between the two columns allows you to drag to change the width of the column.

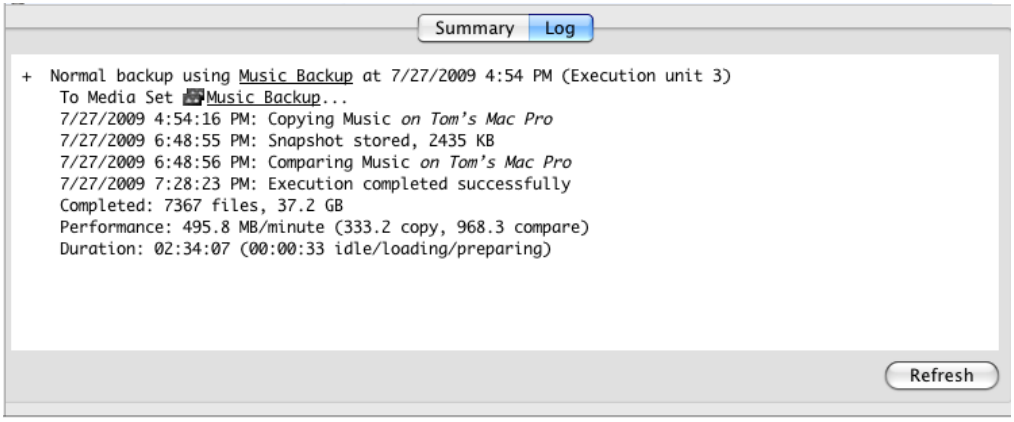
The default columns for the Activity List are Status, Date, Name, Type, Source, Destination, and Performance. Besides these default columns, by right-clicking in any of the column headers, you get a contextual menu from which you may also add additional choices to the list: Activity Thread, Errors, Warnings, Copied Files, Remaining Files, Copied Bytes, Remaining Bytes, and Compression.

Viewing Activity Details

For every activity, Retrospect stores information about the activity in the detail view below the Activity List. For the overview of the activity, click the Summary tab, which shows you information about the activity date, type, what script ran to create the activity, the activity's status, the source and Media Set used, and details on performance and how many files were copied.



Retrospect also stores detailed information about the activity, which you can see by clicking the Log tab.



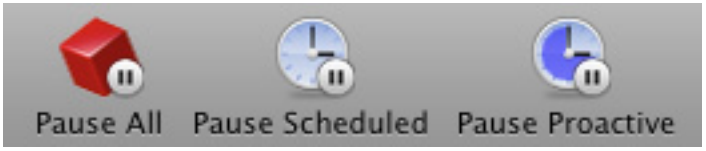
Note: *For currently executing activities, click the refresh button to see the latest information about the activity.*

Pausing Global Retrospect Operations

In some situations, you may wish to pause all or some categories of Retrospect operations. For example, you might wish to hold off scheduled scripts while you are adding or changing hardware on the Retrospect server. Or you

might want to keep Proactive Backups from occurring while you modify the associated script.

Retrospect provides three buttons in the toolbar at the top of the window to allow you to pause different categories of operations. These pause activities are associated with a single Retrospect server; if you have more than one server listed in the Retrospect sidebar, clicking one of the pause buttons will only affect operations on the selected server.



The three buttons have the following effect:

Pause All halts all Retrospect operations; no scripts will execute, and currently running activities will also pause.

Pause Scheduled halts all future operations; no scripts will execute at their scheduled time. Any operations that are currently running will finish as they normally would.

Pause Proactive halts any future Proactive Backup scripts. When Retrospect Clients associated with Proactive Backup scripts appear on the network, Retrospect will not initiate a backup.

To pause Retrospect activities, click on the button corresponding to the kind of activity you wish to pause. When you click one of the buttons, the icon changes from displaying a pause badge to a play badge, and the button's name changes to say Resume instead of Pause. Pause All becomes Resume All; Pause Scheduled becomes Resume Scheduled; and Pause Proactive becomes Resume Proactive. When you are ready to resume activities, click the button again, or click Resume All.

Proactive Backups

Backup scripts are powerful and versatile, but in backup environments that change regularly, another kind of operation—Proactive Backup—may be bet-

ter suited to your needs. A regular backup script copies specific volumes in a certain order to a designated Media Set. If the backup environment changes and volumes or media become unavailable, the backup will not happen until its next scheduled time. This is why Retrospect offers a Proactive Backup option.

Proactive Backup Benefits

Retrospect's Proactive Backups accommodate changing network and disk configurations. A regular backup script follows a rigid schedule for its clearly defined Sources and destination Media Sets. But 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—the volume that was backed up least recently is first to be backed up. The volumes are copied to the best available Media Set media, so Proactive Backup scripts give you greater freedom to use the media of your choice.

Proactive Backup scripts are great for environments in which computers and volumes irregularly appear on the network. For example, in an office that has 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 request early 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, such as for server volumes that need to be backed up at specific times, 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 Retrospect server running the script becomes "proactive" during its scheduled time of operation and is idle during its scheduled period of inactivity. Or if you like, you can set a schedule for the Proactive Backup script that keeps it running all the time.

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.

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 Media 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 early backups of their volumes. This network polling is efficient and does not adversely affect network performance. This whole process ensures that volumes not backed up in the longest amount of time get the next backup.

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 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 "No media action". You can utilize standard backup scripts along with Proactive Backup to perform media actions such as "Skip to new member," "Start new Media Set," and "Recycle Media Set".*

When to use Proactive Backups

The following table includes information comparing standard backup scripts to Proactive Backup Scripts.

Feature	Backup Script	Proactive Backup Script
Destination Media Sets	Copies to a single Media Set as specified in the schedule or at execution. Fails if media is unavailable. Media rotation is scripted.	Copies to the most ideal available Media Set in the destinations list. Automatic media rotation among multiple available Media 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. If a backup fails, Proactive Backup will retry the operation within the specified period of time.
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.

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, if you've chosen to run it at only certain times of the day or night. 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. The volumes that have not been backed up in the longest period of time will always have priority over recently backed up volumes.

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 Smart Incremental backups.

As the backup administrator, you don't 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'll need to allot more backup 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 Rules or Favorite Folders to limit the files to back up, use

a faster Retrospect server, or speed up your network. Providing Retrospect with multiple available Media Set destinations will allow more volumes to be protected from a single copy of Retrospect, as multiple activities will run concurrently. You could also add a second Retrospect server with Proactive Backup handling half of your clients, effectively dividing the load in half for each backup server.

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. Assuming a similar amount of data stored on the computers in each 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 notebook computers. Another script could back them up twenty-four hours a day, because they are available at random times during the day.

Proactive Backup Tips and Techniques

To get the most out of Proactive Backup, you should follow a few simple guidelines.

Use Tags as Sources

Use tags to specify sources in your Proactive Backup scripts, not individual volumes, especially when you back up clients. When you use tags, any new volumes added to a tag are automatically included in backups. If a new client

is given a tag that matches one in your Proactive Backup source list, the client will automatically be backed up without editing that script.

Rotate Among Media Sets

Create multiple Media Sets and use them all as destinations in your Proactive Backup script. Retrospect will automatically make sure each source is prioritized and backed up to the available media that matches one of the destinations in your script.

Introduce New Media

In addition to Proactive Backup scripts, you can use a standard backup script to periodically perform New Media Set backups to introduce new media. Store old media off-site after each New Media Set backup. Between New Media Set backups, periodically perform 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 Media Set backups by executing regular backup scripts using the same Media Sets used by your Proactive Backup scripts. You can schedule these or manually run them from Retrospect's Scripts view.

To manually set a Media Set for a Recycle, configure the Media Set and set the media action.

Monitor Media Availability

Because Proactive Backup does not initially put up media request windows, you have to monitor media from the Activity category of the sidebar. Click Proactive in the Scope Bar to check on your Proactive Backup Scripts.

When Retrospect needs media it displays "media" in the status field of the Activities detail view. Provide media as needed.

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. Other scripts can complement Proactive Backup scripts by starting Recycle and New Media Set backups, and by forcibly backing up volumes that do not get backed up by Proactive Backup. If you have a volume that must be backed up at a specific time, a standard backup script will allow the backup to begin on an exact schedule rather then during the time range of a proactive script.

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 Media Set destinations. Proactive Backup rotates between Media 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 Start New Media Set backup with a standard backup script 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 recent 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 a current backup. Retrospect always polls starting with clients who need backups the most.

Manage User Deferments

When a client user repeatedly defers his or her backups (as indicated in the 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

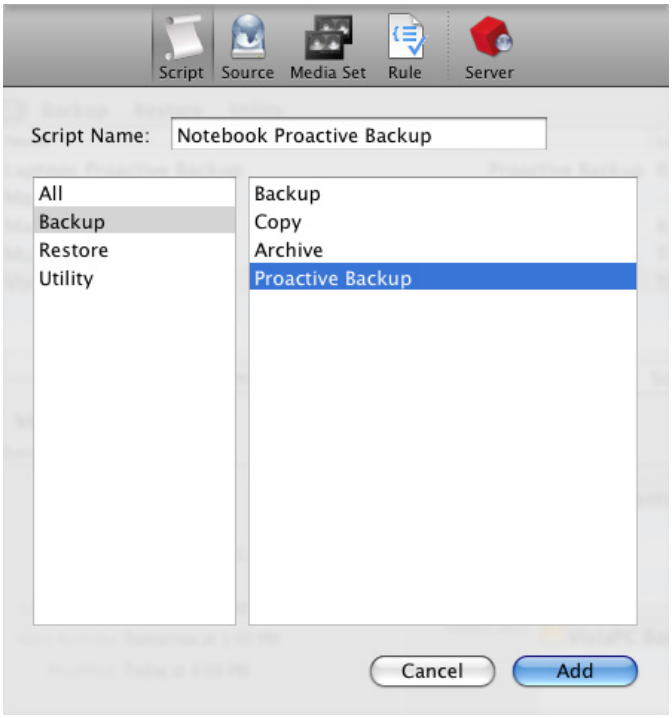
If you find Proactive Backup is not completely backing up all its sources, another way to set the backup priority is by only backing up critical files rather than entire volumes, though you can also do both. Use multiple scripts with different Rules to give some files or folders higher backup priority than others. For example, a higher-priority rule would include documents and settings only, and a lower-priority rule would include all files. Schedule the higher-priority script to run for a longer duration than the lower-priority script.

Creating a Proactive Backup Script

This section takes you through the steps of creating a Proactive Backup script: The process is very similar to manually creating a regular backup script, although Proactive Backup scripts are scheduled differently. There is no Assistant for creating Proactive Backup scripts.

To create a Proactive Backup script, follow these steps:

1. In the Retrospect console's Sidebar, click Scripts. A list of previously created scripts (if any) appears on the right side of the window.
2. In the List View Toolbar, click the Add button. The Script dialog appears.
3. In the Script Name field, enter a name for your new script.

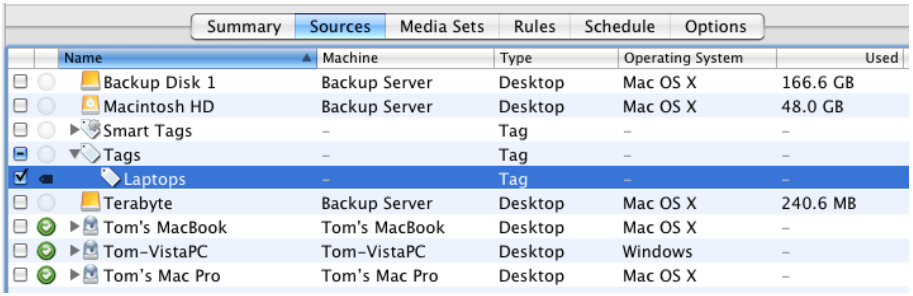


4. Make sure that the All or Backup category is selected, then click Proactive Backup in the script types list on the right side of the dialog, then click Add. The new script appears in the list, with a red icon next to it, indicating that the script is not complete. Below, in the Details area of the Summary tab, you can see that it is blank, telling you that you need to add one or more Sources, Media Sets, and Schedules.

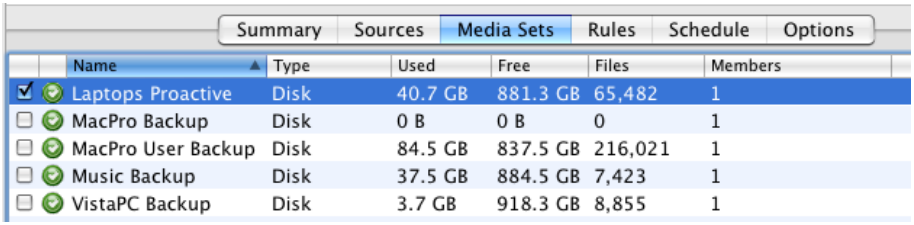
   Note: *If you don't see the source that you need, you must define that source before you can proceed. See Chapters 3 or 4 if you need to know how to add different kinds of sources.*

5. Click on the Sources tab. Retrospect displays the sources that you have already defined. Select the sources that you want to include in the backup by clicking the checkboxes next to them. If necessary, click the disclosure triangles for Retrospect Clients or network shares to see the volumes or Favorite Folders they contain. You may also choose Tags or Smart Tags, which easily groups together multiple Sources. In this

example, that's what we will do, by choosing the Laptops tag we created. When the script executes, any source volume or Favorite Folder that has the Laptops tag applied will be backed up.



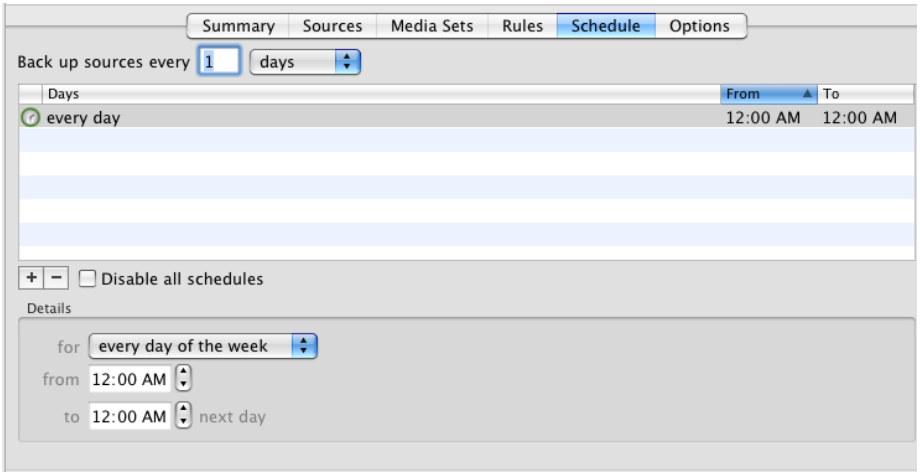
6. Click the Media Sets tab. Retrospect displays the Media Sets that you have already defined. Select the Media Sets that you want as the destination of the backup by clicking the checkboxes next to them. Multiple Media Sets may be selected, allowing the Proactive Backup script to use any and all available backup media.



Note: *You must have defined at least one Media Set before you can proceed. If you need more information, see "Add Media Sets," earlier in this chapter.*

7. Click the Rules tab. Click the radio button next to the Rule that you wish to apply to this backup.

8. Click the Schedule tab. A script has no default schedule, so you must add one by clicking the plus (+) button under the empty schedule list.

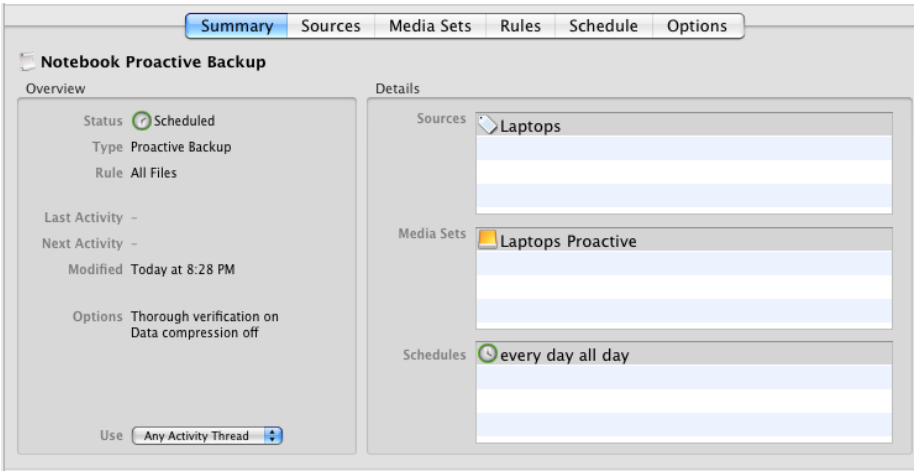


9. In the schedule interface, choose the frequency of the schedule by entering a number in the "Backup sources every" field, then by choosing hours or days from the pop-up menu. In the Details section, from the "for" pop-up menu, choose "every day of the week," "Monday-Friday," "Saturday and Sunday," or "selected days." If you choose this last option, buttons will appear allowing you to choose which days you want the script to run. Finally, choose the time you want to the script to begin execution using the "from" field, and choose the time you want the script to end execution using the "to" field. By default, a Proactive Backup script is set to run every day, all day.

Note: As soon as a Proactive Backup script has a valid source and destination*, its default every-day-all-day schedule will cause Retrospect to begin polling for sources and destinations immediately. Change the script's schedule or use the Pause Proactive button described above if necessary to prevent the Proactive Backup script from running until you are ready.*

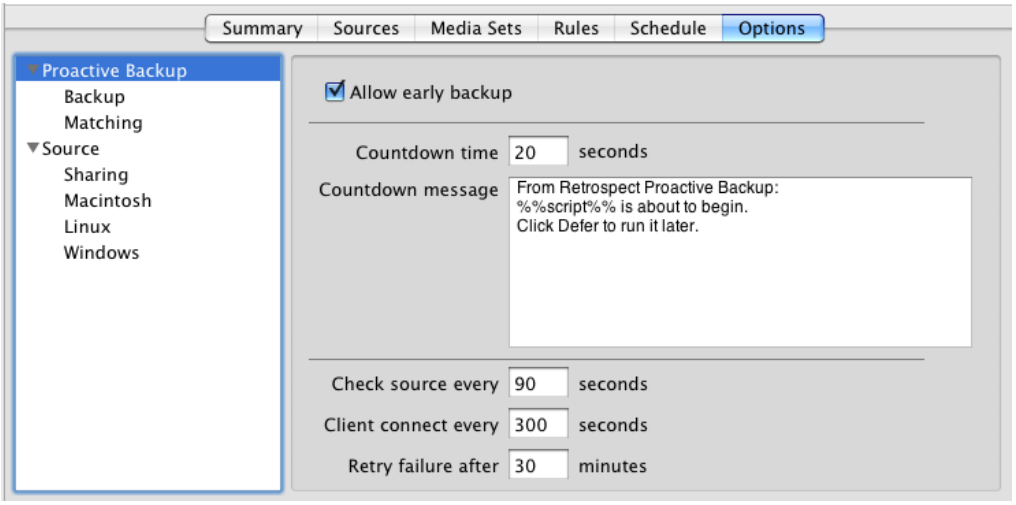
Note: *Just because the Proactive Backup script is scheduled to run all the time, it doesn't necessarily mean that it will be constantly backing up. It will only back up when the source volumes are available and need to be backed up.*

10. Click the Summary tab to review your work. You can now see that Retrospect has all the information it needs to complete the backup.



Proactive Backup Script Options

Most of the options for Proactive Backup scripts are identical to those of regular Backup Scripts, with the exception of the options listed in the Proactive Backup category. For the other options available to Proactive Backup scripts, please refer to “Backup Script Options,” earlier in this chapter.



The specific Proactive Backup options are:

Allow early backup: When this option is on, which is the default, client users may request early backups from their Retrospect Client control panels, overriding the backup frequency. 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 requesting client's source volumes.

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. When Retrospect's Proactive Backup script goes to back up 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. Enter zero to make Retrospect skip the countdown notification entirely.

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.

There are also three options that control how often the Retrospect Server will poll the Clients for volumes that need to be backed up:

Check source every *n* seconds: Retrospect uses this time interval, which is 90 seconds by default, to check whether a source is available for backup.

Client connect every *n* seconds: Retrospect uses this time interval, which is five minutes (300 seconds) by default, to access a client to check whether the user has changed the backup schedule or requested an early backup.

Retry failure after *n* minutes: 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.

Copying

A Copy operation copies the selected files in their native file format from one drive or folder to another. After a copy operation, the destination drive contains an exact copy of every file and folder that was copied. You can open, edit, and otherwise work with the files. Files and folders are copied without compression (which is an option for Backup operations). Previous versions of Retrospect called Copy operations Duplicate operations.

Warning: *When you copy all files and folders from one disk to another, Retrospect deletes any data that may already be on the destination volume. Be careful!*

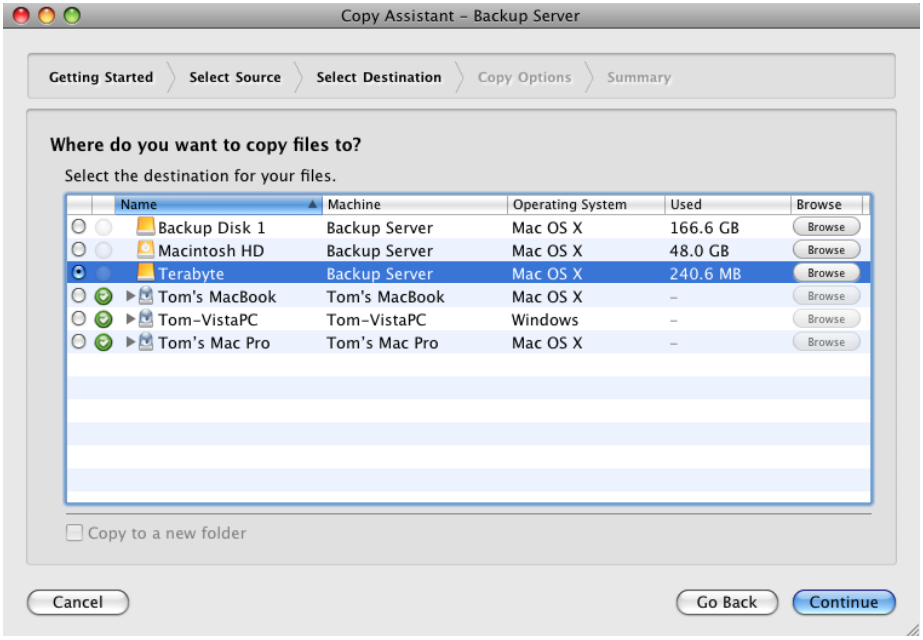
Using the Copy Assistant

Using the Copy Assistant, you can choose to copy an entire volume to a destination volume (you might want to do this to create a bootable copy of a Macintosh startup disk, which is the kind of copy used in this example) or copy selected files or folders.

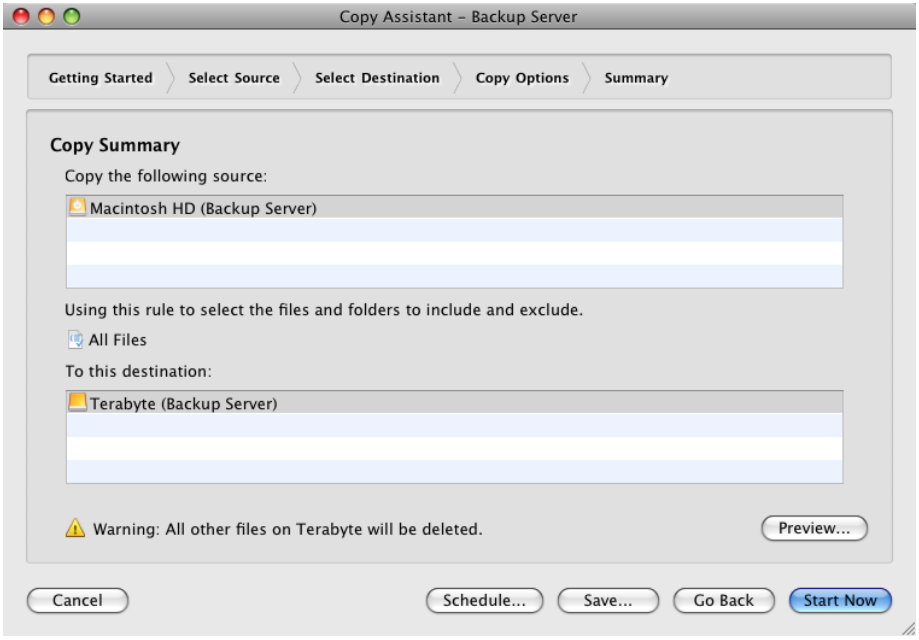
To create a copy script with the Copy Assistant, copying one hard drive to another:

1. Click the Copy button in the Toolbar. The initial Copy Assistant window appears, asking you if you want to copy an entire volume or folder, or select files and folders to copy. Click “Make an exact copy of the source volume or Favorite Folder,” then click the Continue button. The Select Source pane appears.

2. Click the radio button next to the source that you want to copy. You may also apply a rule to the Copy operation, but in this case, because we want to create an exact duplicate of the source volume, the All Files default choice makes sense. Click the Continue button. The Select Destination pane appears.



3. Click the radio button next to the destination for the copy, then click Continue. You can choose any volume Retrospect has listed in Sources, but the root of a disk must be selected if you wish to make a bootable copy as described in this example. If you do not care about making a bootable copy, and you want to prevent Retrospect from overwriting files that already exist on the destination volume, select an empty Favorite Folder as the destination. All items outside of that folder will be left untouched by the copy operation. The Summary screen appears, recapping the source and destination of the copy. If you want to immediately run the copy script, click Start Now.



Note: *For an external disk to be bootable after a copy operation, the "Ignore ownership on this volume" Finder option must be unchecked before starting your copy process. This option is found by doing a Get Info in the Finder on the disk to which you are copying. Consult Apple's help documentation on the correct volume format required to be bootable with your specific Macintosh configuration*

4. (Optional, but recommended) Click the Save button to display a dialog where you can give the script a name. If you do not, Retrospect will name the script "Copy Assistant date and time created," which may make it difficult to later tell at a glance the purpose of the script. Enter the script name, then click Save to return to the Copy Assistant's Summary screen.

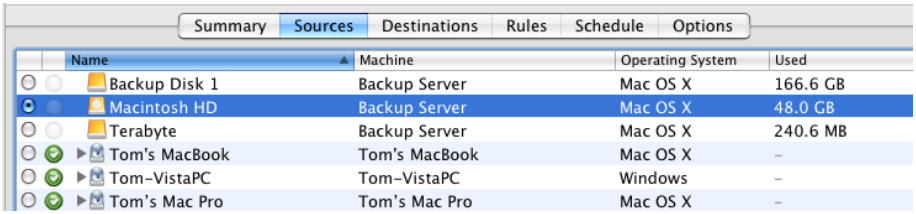
5. (Optional) If you would like to set up a schedule for the script to run at a later time, click the Schedule button. The Assistant changes to the scheduling interface, with a default schedule set. When you're done setting up the schedule that you want, click Start Now, which saves the script and its schedule. The script will run automatically at the date and time you specified.

Creating a Copy Script Manually

Creating a Copy script manually is much like creating a Backup script. The differences are that where a Backup script uses Media Sets as a destination for the backed up files and folders, the Copy script uses volumes as a destination for the data, and calls them, sensibly, Destinations. There are options within the Copy script's Destinations tab that allows you to fine tune the way Retrospect does the copy.

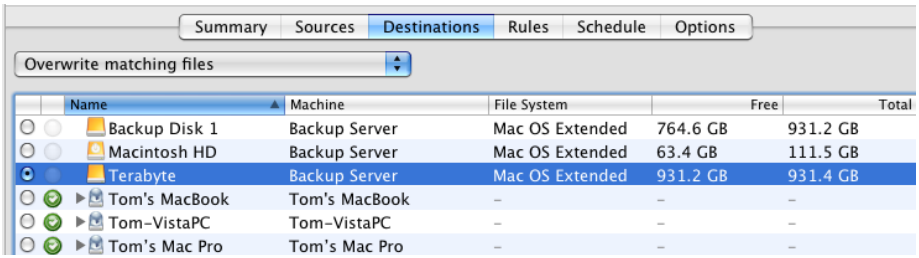
To create a Copy script manually, follow these steps:

1. In the Retrospect console's Sidebar, click Scripts. A list of previously created scripts (if any) appears on the right side of the window.
2. In the List View Toolbar, click the Add button. The Script dialog appears.
3. In the Script Name field, enter a name for your new Copy script.
4. Make sure that the All or Backup category is selected, then click Copy in the script types list on the right side of the dialog, then click Add. The new script appears in the list, with a red icon next to it, indicating that the script is not complete. Below, in the Details area of the Summary tab, you can see that it is blank, telling you that you need to add one or more Sources, Destinations, and Schedules.
5. Click the Sources tab. Retrospect displays the Sources that you have already defined. Select the Source you want to copy by clicking the radio button next to it. By the nature of the copy operation, you may only copy one Source to one Destination. The source can be a volume or a Favorite Folder from a volume.



6. Click the Destinations tab. Retrospect displays the Sources that you have already defined. Select the destination of the backup by clicking

the radio button next to it. The destination can be a volume or a Favorite Folder from a volume.



The Destinations tab has a pop-up menu with several copying options. Choose the option you want:

Overwrite entire volume replaces the entire contents of the destination volume or Favorite Folder with the selected files and folders from the source volume or Favorite Folder. Everything else on the destination volume is deleted. Retrospect saves time by not copying identical files, that is, files that share the same location, name, modification date and time, etc., that are already present on the destination. New files are added, and different versions of files already present on the destination are replaced by the files from the source, even if the file already present on the destination is newer.

Overwrite matching files works exactly like "Overwrite entire volume" above, with one important difference: Files and folders that already exist on the destination volume but that aren't present on the source volume are not deleted from the destination. This means that if a file that exists on both the source and destination is deleted from the source before an "Overwrite matching files" Copy script is run, the copy operation won't remove that file from the destination. This is the default option.

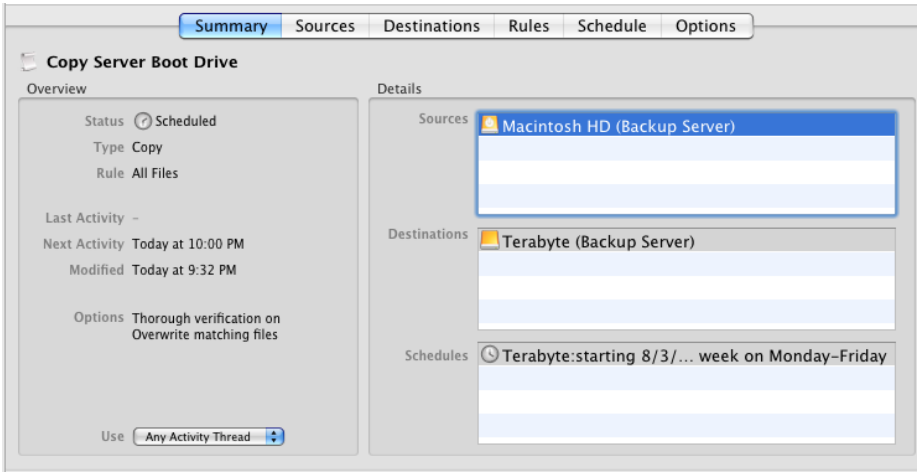
Overwrite older files copies the selected files and folders to the destination volume. When Retrospect finds a file that exists on both the source and destination, the destination file is overwritten only if the source file is newer.

Copy only missing files copies the selected files and folders to the destination volume. When Retrospect finds a file that exists at the same

location on both the source and destination, Retrospect leaves those files untouched. No files are deleted from the destination.

Copy to a new folder copies the selected files and folders to a new folder on the destination volume. Other files and folders on the destination are left untouched.

7. Click the Rules tab. Click the radio button next to the Rule that you wish to apply to this copy operation. For more information about Rules, see Chapter 7.
8. Click the Schedule tab. A script has no default schedule, so you must add one by clicking the plus (+) button under the empty schedule list.
9. In the schedule interface, the Destination pop-up menu lists the Destination that you previously set. Finally, set the date, time, and frequency for the Schedule to execute. See "Working with Schedules," later in this chapter, for more information.
10. Click the Options tab, then set the copy script options you desire. See "Copy Script Options" for more information.
11. Click the Summary tab to review your work. You can now see that Retrospect has all the information it needs to complete the backup.



Copy Script Options

Copy scripts share most of their options with backup scripts. See "Backup Script Options," earlier in this chapter. The Copy script options are:

Move files 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.

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

On Move, don't delete empty folders keeps folders that become empty as a result of the move instead of automatically deleting them. By default, this option is off.

Recompute icon positions 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.

Ignore encrypted file verification errors causes Retrospect to ignore verification errors with encrypted files on NTFS volumes, preventing the Log from being filled with errors that can typically be ignored, as they result from valid changes made by the file system during the copy process.

Ignore file verification errors in security stream causes Retrospect to ignore verification errors with security streams on NTFS volumes, preventing the Log from being filled with errors that can typically be ignored, as they result from valid changes made by the file system during the copy process.

Archiving

Archiving lets you copy files from a volume to a Media Set for off-line storage. Archiving allows you to remove seldom-used files from a hard disk while

maintaining a copy of those files on your storage media. With archive scripts, you can choose to move—rather than just copy—files from the source to the destination. For example, you might want to move the files for a particular project off your main hard disk after the project is completed, but still have those files be easily findable if you ever need to refer to them.

Note: *An archive script has one major difference from a backup script. Archiving has the matching options disabled by default so that all files from the source are copied, even if they have previously been copied to the same Media Set. This is done for two reasons. By placing all the files belonging to an archived project together on the backup media, Retrospect ensures the fastest restore of the archived files. Additionally, when the "Delete source files after copying and verifying" option is selected, only files archived and verified during that session will be deleted from the source.*

As with backups, there are three basic steps in archiving:

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

Creating an Archive Script

To create an Archive script, follow these steps:

1. In the Retrospect console's Sidebar, click Scripts. A list of previously created scripts (if any) appears on the right side of the window.
2. In the List View Toolbar, click the Add button. The Script dialog appears.
3. In the Script Name field, enter a name for your new Archive script.
4. Make sure that the All or Backup category is selected, then click Archive in the script types list on the right side of the dialog, then click Add. The new script appears in the list, with a red icon next to it, indicating that the script is not complete. Below, in the Details area of

the Summary tab, you can see that it is blank, telling you that you need to add one or more Sources, Media Sets, and Schedules.

5. Click the Sources tab. Retrospect displays the Sources that you have already defined. Select the Source you want to copy by clicking the checkbox next to it. You may choose more than one Source.

   Note: *If you want to archive a folder on your hard disk, you must have already set it up as a Favorite Folder in Retrospect's Sources.*

6. Click the Media Sets tab. Retrospect displays the Media Sets that you have already defined. Select the destination of the archive by clicking the checkbox next to it.

   Tip: *You can archive to more than one Media Set, using different schedules to make the archive to each set.*

7. Click the Rules tab. Click the radio button next to the Rule that you wish to apply to this backup. For more information about Rules, see Chapter 7.

8. Click the Schedule tab. An Archive script has no default schedule, so you must add one by clicking the plus (+) button under the empty schedule list.

9. In the schedule interface, the Destination pop-up menu lists the Media Set(s) that you previously set. Choose the Media Set that you want. Finally, set the date, time, and frequency for the Schedule to execute. See "Working with Schedules," later in this chapter, for more information. Note that archive scripts do not give you a choice of media action like you will find in a backup script. The archive script always appends files to the destination Media Set.

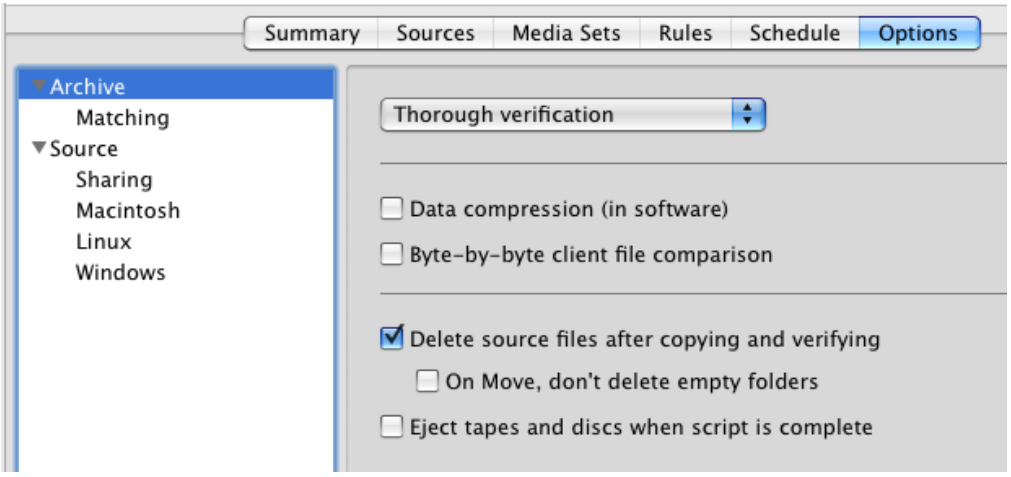
   Tip: *If you use archiving to move files (see the Move files option for Copy scripts above), it is recommended that you disable grooming for Disk Media Sets containing archived files so that no data will accidentally be deleted.*

10. Click the Options tab, then set the archive script options you desire. See "Archive Script Options" for more information.

11. Click the Summary tab to review your work. You can now see that Retrospect has all the information it needs to complete the backup.

Archive Script Options

Most of the options for Archive scripts are identical to those of regular Backup and Copy scripts, with the exception of some of the options listed in the Archive category. For the other options available to Archive scripts, please refer to "Backup Script Options" and Copy Script Options," earlier in this chapter.



The specific Archive options are:

Delete source files after copying and verifying causes Retrospect to copy the selected files and folders, verify that the copy is good, and then erase the source files. In effect, the selected files and folders are moved from the source volume to the archive Media Set.

On Move, don't delete empty folders prevents Retrospect from erasing the empty folders after it has copied, verified, and deleted the files within them.

Restoring

Retrospect allows you to restore an entire volume (which can be a source or Favorite Folder), or selected files and folders, from the most recent backup

or any previous backup. Retrospect makes it easy to restore an entire volume, a folder, or a selected file to its exact state as of a given point in time. Every time Retrospect performs a Smart Incremental backup of a volume, it saves a list of all the files and folders present at that point in time (like a snapshot, along with all their corresponding attributes and permissions) and saves it in the Catalog and on the Media Set along with the backup. Each time a backup runs, Retrospect saves an updated listing. When you need to restore an entire volume, you merely need to select the backup you want. Most of the time, but not always, this will be the most recent backup. Retrospect will use that point-in-time listing to know exactly which files need to be restored.

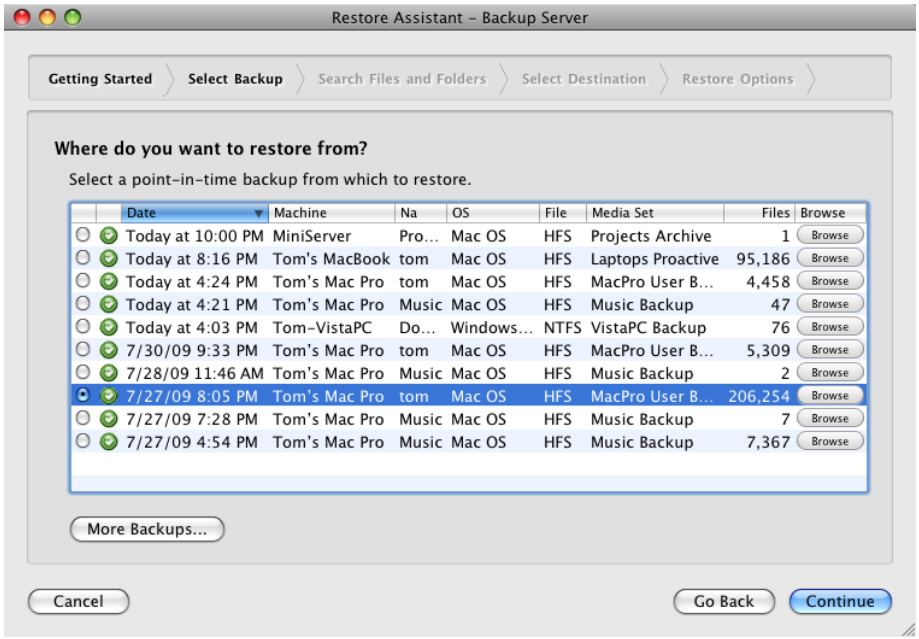
For the fastest restores, Retrospect uses its matching and Smart Incremental technologies to only restore files that don't exactly match those already present on the destination. This allows you to "roll back" a volume or Favorite Folder to a previous point in time by only restoring the files that are different and then deleting files that no longer belong on the destination.

Using the Restore Assistant to Restore an Entire Drive

To create a restore script with the Restore Assistant, restoring an entire drive:

1. Click the Restore button in the Toolbar. The initial Restore Assistant window appears, asking what sort of restore you want to perform.

2. Choose “Restore an entire source volume or Favorite Folder to a previous point in time,” then click Continue. The Select Backup pane appears.



3. Choose the backup that reflects the point in time to which you want to restore. If you have many backups, you may find it easier to sort the list by Machine or Media Set. To do that, click the heading of the column by which you want to sort. Click the heading again to reverse the sort order. When you have found and selected the backup you want, click Continue. The Select Destination pane appears.

   Click the radio button next to the name of the destination volume, then click Continue. The Restore Options pane appears, recapping the source and destination of the copy.

   Warning: *This sort of restore will delete all other files on the destination volume. Be careful!*

4. When you are ready to perform the restore, click Start Now.

Using the Restore Assistant to Find and Restore Files and Folders

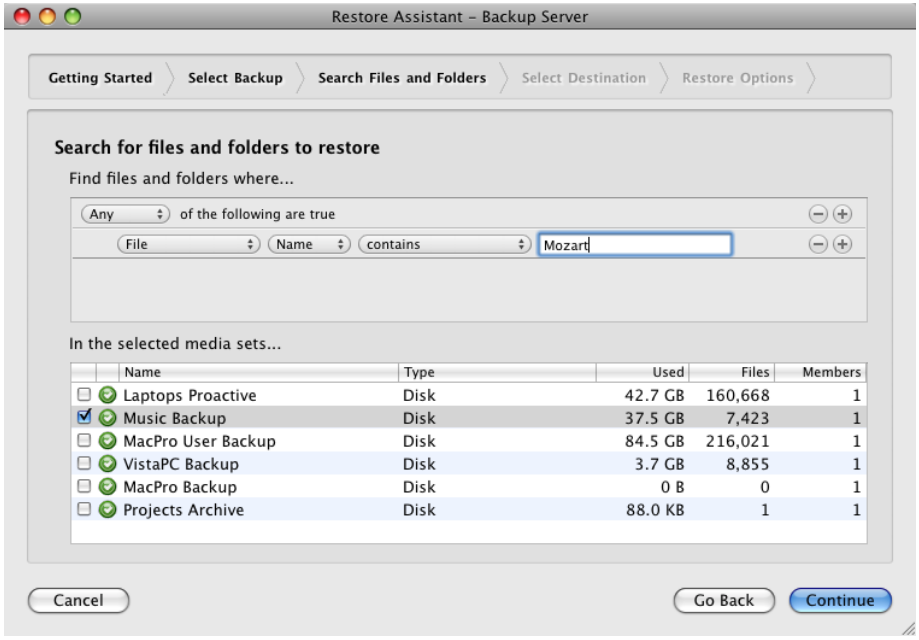
Sometimes you only want to restore particular files or folders from a backup or archive. For example, imagine that a client contacts you, requesting that you go back to a point in their project before the last round of changes was made. You'll need to retrieve the project files for that point in time from the backup media. Retrospect allows you to select certain files and folders to be restored, or to search across your Media Sets for files and folders that match particular criteria.

To find and restore particular files or folders:

1. Click the Restore button in the Toolbar. The initial Restore Assistant window appears, asking what sort of restore you want to perform. Depending on what you want to do, choose "Restore selected files and folders" or "Search for files in the selected media sets," then click Continue. The Select Backup pane appears.
2. If you chose "Restore selected files and folders" in step 1, the Select Backup pane will allow you to select a point-in-time backup. Do so, then click the Browse button for that backup. If the selected backup contains a large number of files, it may take some time for Retrospect to display its files and folders. In the resulting dialog, navigate to and select the files and folders that you wish to restore, then click the Select button. You will be returned to the Select Backup pane. Click Continue.

   or

   If you chose "Search for files in the selected media sets" in step 1, the Select Backup pane will display a search interface. In the part of the pane labeled "Find files and folders where," select and enter the criteria that you want using the pop-up menus and text entry fields. To add or subtract additional criteria, click the plus (+) or minus (-) buttons, respectively, just as you would using the Finder's Find command.

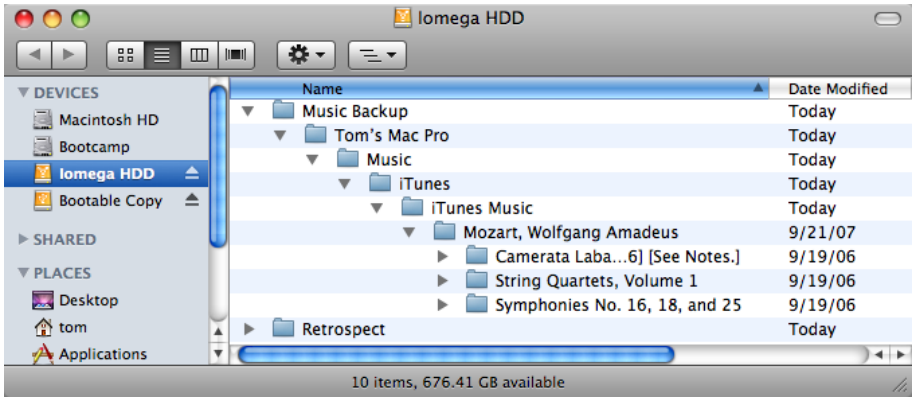


In the part of the pane labeled “In the selected media sets,” click the checkbox next to the Media Set you want to search, then click Continue.

3. The Select Destination pane appears. You will also usually want to click the “Restore to a new folder” checkbox. Click Continue.

4. The Restore Options pane appears. If the results of your search criteria are found in more than one backup, you may select files and folders from multiple backups and multiple Media Sets. Click Continue.

5. The Restore Summary pane appears, recapping the source and destination of the restore operation. Click Start Now to begin the restore. When the restore finishes, you will find the results in a new folder on the destination, one for each Media Set from which files were restored, with the folder structure of the original source preserved within those folders. Any new folders created will have the same names as the Media Sets that contained the backed up files.

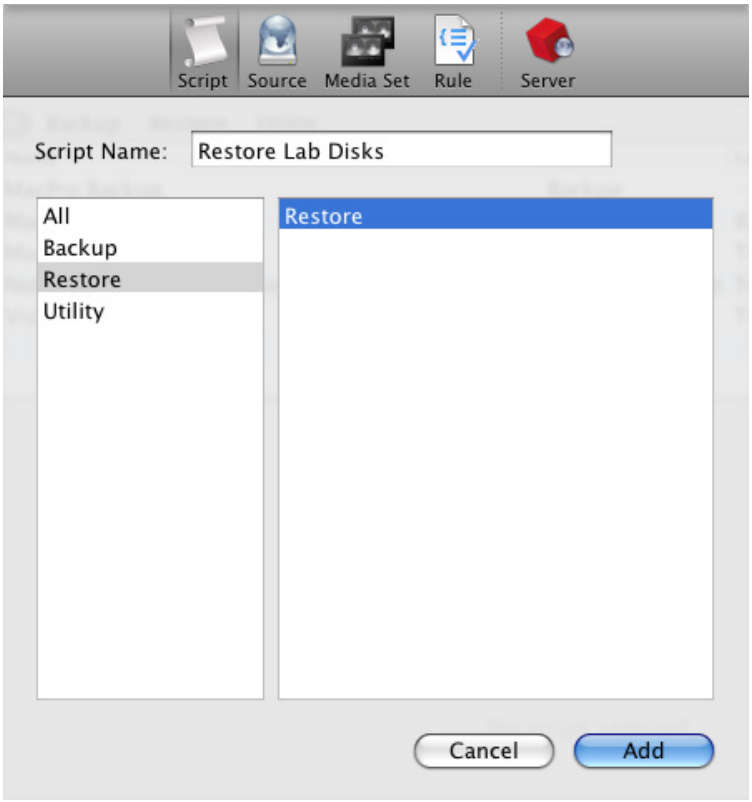


Creating a Restore Script Manually

Most of the time, Restore operations are performed ad-hoc (you want to restore some archived files, or bring back a copy of a corrupted file), and the Restore Assistant does a fine job of walking you through such operations. 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, rolling them back to a clean state.

To create a restore script:

1. In the Retrospect console's Sidebar, click Scripts.
2. In the List View Toolbar, click the Add button. The Script dialog appears.
3. In the Script Name field, enter a name for your new Restore script.
4. Make sure that the Restore category is selected, then click Restore in the script types list on the right side of the dialog, then click Add. The new script appears in the list, with a red icon next to it, indicating that the script is not complete. Below, in the Details area of the Summary tab, you can see that it is blank, telling you that you need to add one or more Backups, Destinations, and Schedules.



5. Click the Backups tab. Retrospect displays a list of the previous backups. Select the backup you want to restore by clicking the radio button next to it.

6. Click the Destinations tab. Retrospect displays a list of the volumes defined in Sources. Select the destination for the restore by clicking the radio button next to it. There are also five options available from a pop-up menu in this tab. Choose one of these:

   Restore entire volume makes the destination volume exactly match the source backup. It deletes all files and folders on the destination that do not match those marked for restore in the backup, leaving files untouched if they are identical to files marked for restore. It then copies all remaining files and folders from the backup to the destination, preserving the folder hierarchy.

Overwrite corresponding files restores all selected files from the backup that do not exist on the destination and overwrites corresponding files on the destination that also exist in the source backup. These "corresponding" or "matching" files on the destination are always overwritten with files from the backup regardless of whether the backed-up 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.

Overwrite older files restores all selected files from the backup that do not exist on the destination and overwrites matching files on the destination only if the backed-up file is newer than the destination file.

Restore only missing files restores all selected files from the backup that do not exist on the destination, but does not overwrite any files on the destination. Matching files on the destination are left untouched.

Restore to a new folder restores all selected files from the backup to a new folder on the destination. This folder will have the same name as the Media Set used for the restore.

7. Click the Rules tab. Click the radio button next to the Rule that you wish to apply to this backup.
8. Click the Schedule tab. A Restore script has no default schedule, so you must add one by clicking the plus (+) button under the empty schedule list.
9. In the schedule interface, the Destination pop-up menu lists the volume that you previously set. Finally, set the date, time, and frequency for the Schedule to execute. See "Working with Schedules," later in this chapter, for more information.
10. Click the Options tab, then set the restore script options you desire. See "Restore Script Options" for more information.

Restore Script Options

Many restore script options are identical to the backup script options. See "Backup Script Options," earlier in this chapter, for details on options not listed here. The specific restore script options are:

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.

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 System State For Windows machines, Retrospect restores registry and System State information from the backup (if the destination is a bootable system volume).

Working with Schedules

Although you can manually execute a script at any time by selecting it in the Scripts list and clicking the Run button in the toolbar, 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.

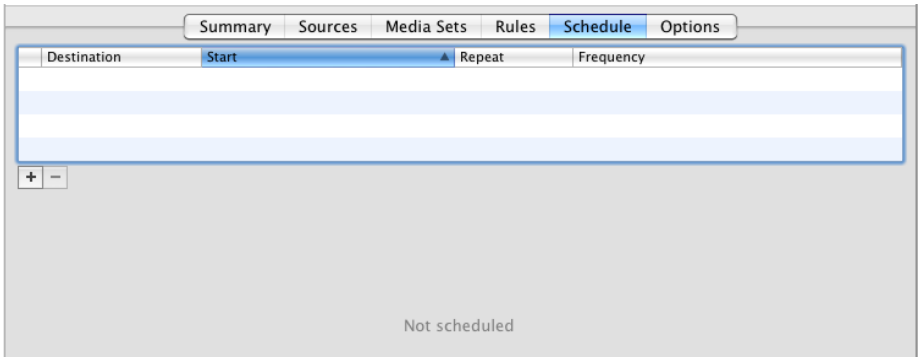
You can schedule a script to run automatically on specified days or on a repeating schedule, such as every two weeks. You can define multiple schedules for the same script and specify the kind of backup you want for each scheduled execution.

Creating a Schedule

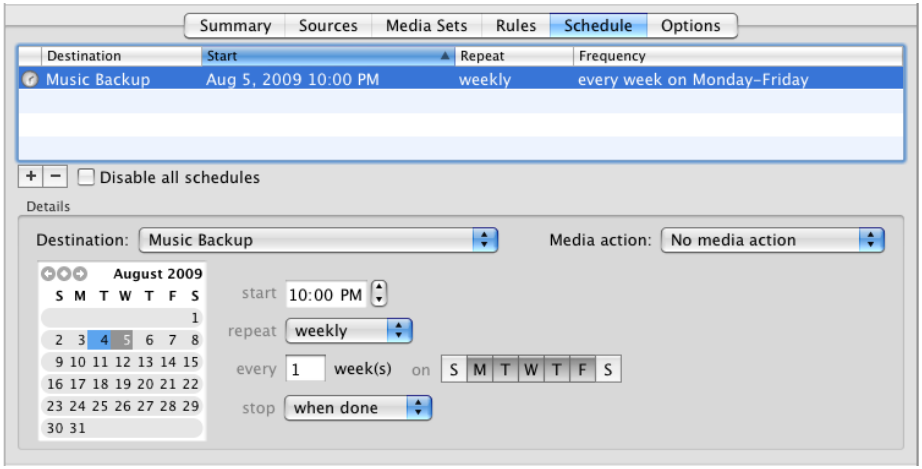
To create a schedule, you must first be working with a script. Throughout this chapter, instructions refer you to this section, which will focus on the specific options you have when creating a schedule.

To create a schedule, follow these steps:

1. In the Detail view of any script, click the Schedule tab. All scripts begin with no schedule, except for Proactive Backup scripts, which are assigned a default schedule of every day, all day.



2. Click the Plus (+) button at the bottom of the schedules list. The bottom of the detail view changes to show the Schedule interface, which defaults to a schedule that runs Monday through Friday at 10 PM. If this schedule suits you, you're done.



3. The Destination pop up menu allows you to choose between the different Media Sets that you have selected to be used with this script (you do this in the Media Sets tab of the script). Some script types allow only one Media Set to be specified, so that one will be the only choice for the menu.

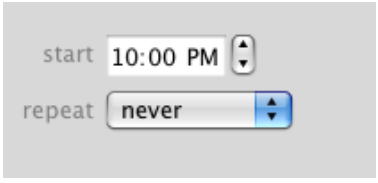
4. The Media action pop-up menu gives you a choice of "No media action," "Skip to new member," "Start new Media Set," or "Recycle Media Set." See Chapter 2 for more information about these media actions.

5. In the calendar, click the start date for the schedule. The current date is shown with a blue highlight, and the start date you choose is shown with a gray highlight.

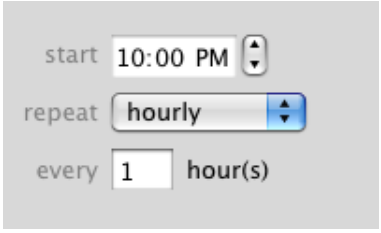
6. In the start field, choose the time you want the script to execute. You may type numbers in this field, or you can click into the field and use the up and down arrows on your keyboard to change the hours, minutes, and AM/PM settings.

7. From the repeat pop-up menu, choose never, hourly, daily, weekly, or monthly. The rest of the schedule interface changes, depending on the choice that you make. Above, in the schedule list, the start, repeat, and frequency columns will change as you modify the settings below, allowing you to easily see the effects of your changes.

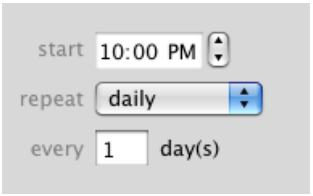
   Repeat never tells the script to execute only once, at the date and time specified.



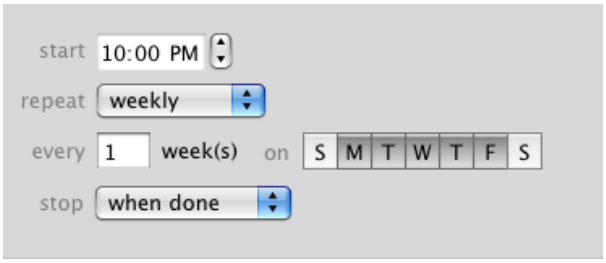
   Repeat hourly tells the script to execute every hour, at the specified time.



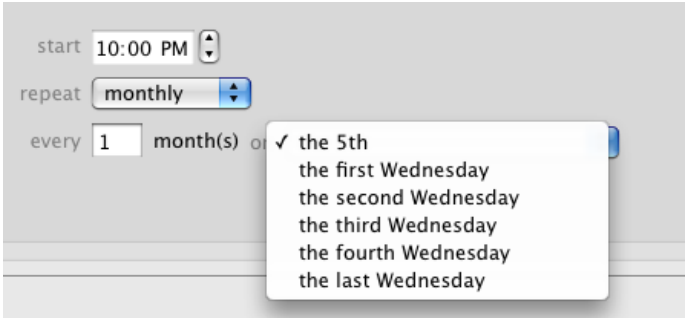
   Repeat daily tells the script to execute once per day, at the specified time.



Repeat weekly tells a script to execute every *n* week(s), at the specified time, on the days that you select using the Sunday through Saturday buttons, and to stop the backup either when it is done or at a fixed time which you can also set. The default value is 1, which tells Retrospect to repeat every week. Setting this value to 2 would repeat every other week.



Repeat monthly tells the script to execute every *n* month(s), at the specified time, and on either a particular date each month or on either the first, second, third, fourth, or last day of the week within the month (which day depends on what day of the week you have chosen in the calendar as your start date).



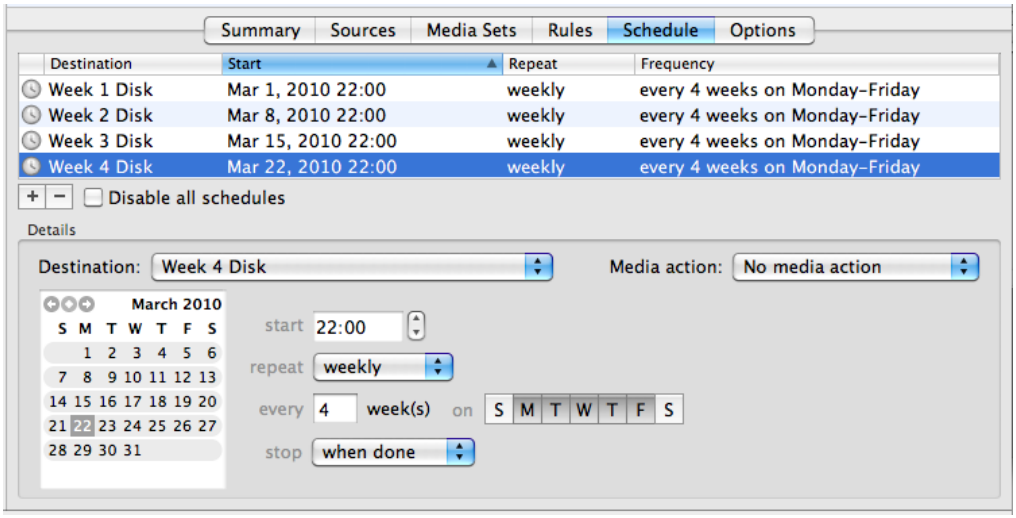
Disabling schedules for a script

Sometimes you want to keep a script from executing. For example, if you have a backup script that has several sources, and you know some of those sources will be off-line at the backup time, you can disable the schedule until all of the sources are available. If you want to keep a particular script from executing, go to the Schedule tab for that script and select the "Disable all schedules" checkbox under the schedule list.

Working with multiple schedules

There are many reasons why you might want to add multiple schedules to a single script. For example, say that you have one schedule that does a daily backup to Media Set A using the "No media action" setting. You can have a second schedule that backs up the same sources, but only backs up once a month, to Media Set B that you use as your off-site backup. A third schedule could then use the "Recycle Media Set" action on Media Set A, resetting the Media Set's contents to control how much media space Media Set A uses.

Another possibility would be to use different schedules to rotate your back-ups among different Media Sets. For example, imagine that you have five Media Sets, one for each day of the work week, Monday through Friday. You can then create five corresponding schedules. The first schedule would repeat weekly, would execute every Monday, and its destination would be the Monday Media Set. You would then create similar schedules for each succeeding day of the week.



As you can see, by using multiple schedules, you can design your backup strategy to cover almost any need.

Working with Utility Scripts

Besides the workhorse scripts covering backup, restore, and copying, Retrospect has several script types for special operations, which are called utility scripts. There are four utility script types:

Copy Media Set makes a copy of the backed up data contained in a source Media Set to a specified destination Media Set. This kind of script copies only those unique files not already contained in the destination Media Set, along with the file/folder listings and metadata for every backup contained in the source Media Set. You can use this script to clone a Media Set, protect against media failure, copy a Media Set for off-site storage, or consolidate backups from multiple Media Sets to a single Media Set.

Copy Backup scripts allow you to copy one or more backups from one Media Set to another Media Set. Retrospect provides you with the ability to copy most recent backups, selected backups, or all backups. You can use this script to copy the most recent backup of each source to a new Media Set for offsite storage or to create a virtual full backup of an entire network of computers.

Verify scripts allow you to verify that the contents of a Media Set were accurately written to the destination media.

Groom scripts provide the ability to schedule a time to reclaim disk space for Disk Media Sets.

You create utility scripts in much the same way that you create any other Retrospect script.

Creating a Copy Media Set Script

Copy Media Set scripts, by default, match files in the source to files already in the destination and only copy the necessary files, that is, those not already present in the destination. This script is additive by default; existing backups already on the destination remain untouched.

To copy files between Tape Media Sets, you must have a separate tape drive for each Media Set, even if both Media Sets are on the same type of physical media. In the case of Disk and File Media Sets, the need for separate backup devices does not apply, provided the drives containing the Media Sets in use for the script are all connected and available.

Tip: *If you do not have separate drives for each Media Set, you can first copy files temporarily to a Disk Media Set and then copy the Disk Media Set to the final destination Media Set.*

To create a Copy Media Set script, follow these steps:

1. In the Retrospect console's Sidebar, click Scripts.
2. In the List View Toolbar, click the Add button. The Script dialog appears.
3. In the Script Name field, enter a name for your new Copy Media Set script.
4. Make sure that the Utility or All category is selected, then click Copy Media Set in the script types list on the right side of the dialog, then click Add. The new script appears in the list, with a red icon next to it, indicating that the script is not complete. Below, in the Details area of

the Summary tab, you can see that it is blank, telling you that you need to add one or more Sources, Destinations, and Schedules.

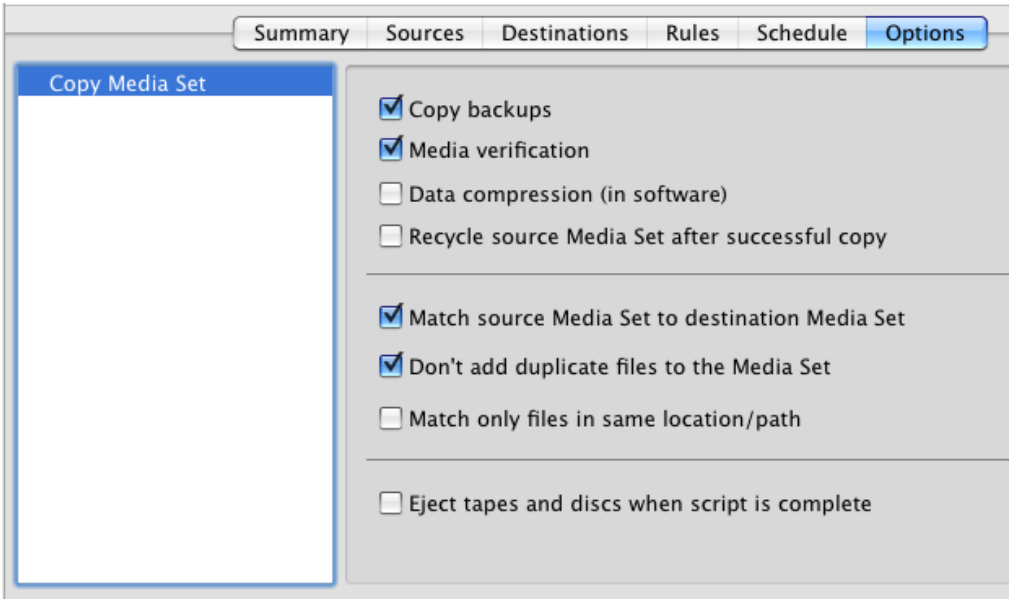
5. Click the Sources tab. From the list of Media Sets, choose one or more by clicking the checkboxes next to them.

   Tip: *By checking more than one Media Set, you can consolidate multiple sets into a single destination Media Set.*

6. Click the Destinations tab. Choose the destination Media Set by clicking the radio button next to it. You may only choose a single destination Media Set.
7. Click the Rules tab. Select the rule you want to apply to the backup.
8. Click the Schedule tab. If you want the Copy Media Set script to execute at some regular interval, click the Plus (+) button to create a schedule, then set the schedule's options. You do not have to set a schedule for the script; you might prefer not to, if this utility script will only need to be run occasionally, you can execute it manually by clicking the Run button in the toolbar.
9. Click the Options tab, then set the script options you desire. See "Copy Media Set Script Options" for more information.

Copy Media Set Script Options

Many of the options for Copy Media Set scripts are identical to those of regular Backup Scripts. This section lists only the ones unique to this kind of script. For the other options available to Copy Media Set scripts, please refer to "Backup Script Options," earlier in this chapter.



The specific Copy Media Set script options are:

Copy backups: This copies the point-in-time file and folder listings and information about those files along with any metadata required to provide point-in-time restores from the destination Media Set. Deselecting this option will only copy the files contained in the source Media Set, and the destination Media Set will lack the necessary file/folder listings and metadata to perform complete point-in-time restores.

Media verification: This option uses MD5 digests generated during the copy to verify files on the destination Media Set.

Recycle source Media Set after successful copy: This option deletes the contents of the source Media Set's Catalog and prepares its media to be overwritten if the script completes with no errors.

Warning: *If enabled, this option will delete all the data in the source Media Set. Be careful!*

Creating a Copy Backup Script

If you need to copy backups and their associated metadata from their source Media Sets to a new or existing Media Set on a regular basis, you can create a Copy Backup script to automate the process. These scripts can be used to:

- Start a new Media Set
- Create an offsite disaster recovery Media Set
- Start a new cycle of backups with a virtual full backup

Copy Backup scripts are different from Copy Media Sets scripts in a number of ways:

- They copy only active backups; Copy Media Sets scripts copy all backups.
- They provide different methods for selecting which backups get copied, such as the most recent backup for each source contained in the source Media Set; Copy Media Sets scripts always copy all backups.

By default, copying backups matches files in the source to files already in the destination and only copies the necessary files. Existing backups and point-in-time file/folder listings already present on the destination Media Set remain untouched.

To copy files between Tape Media Sets, you must have a separate tape drive for each Media Set, even if both Media Sets are on the same type of media. In the case of Disk and File Media Sets, the need for separate backup devices does not apply.

Tip: *If you do not have separate drives for each Media Set, you can first copy files temporarily to a Disk Media Set and then copy the Disk Media Set contents to the final destination Media Set.*

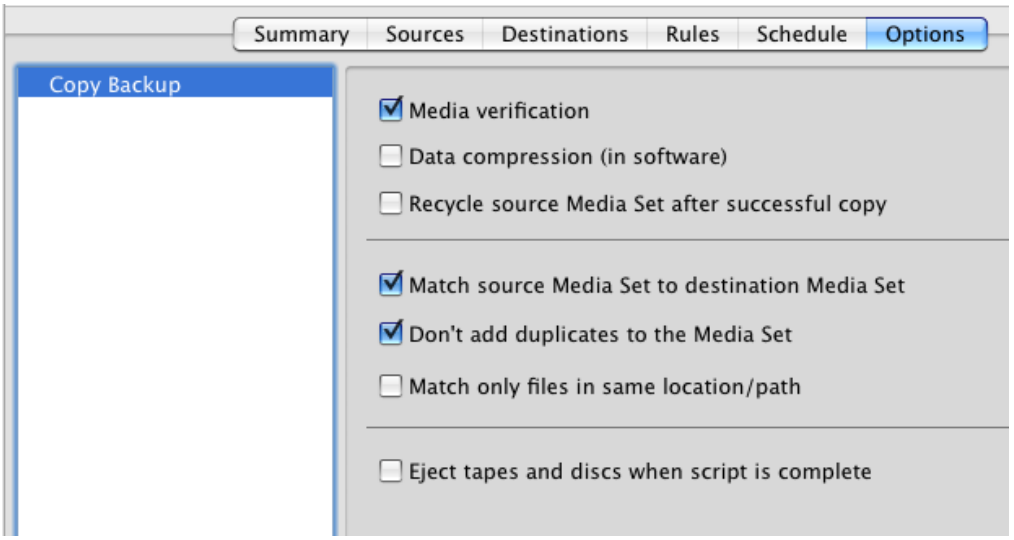
To create a Copy Backup script, follow these steps:

1. In the Retrospect console's Sidebar, click Scripts.
2. In the List View Toolbar, click the Add button. The Script dialog appears.
3. In the Script Name field, enter a name for your new Copy Backup script.

4. Make sure that the Utility or All category is selected, then click Copy Backup in the script types list on the right side of the dialog, then click Add. The new script appears in the list, with a red icon next to it, indicating that the script is not complete. Below, in the Details area of the Summary tab, you can see that it is blank, telling you that you need to add one or more Sources, Destinations, and Schedules.
5. Click the Sources tab. From the list of Media Sets, choose one by clicking the radio button next to it. Then from the pop up menu, choose the backups you want to make part of the copy:
   - Copy most recent backups for each source
   - Copy most recent backups for each selected source
   - Copy selected backups
   - Copy all backups
6. Click the Destinations tab. Choose the destination Media Set by clicking the radio button next to it. You may only choose a single destination Media Set.
7. Click the Rules tab. Select the rule you want to apply to the backup.
8. Click the Schedule tab. If you want the Copy Backup script to execute at some regular interval, click the Plus (+) button to create a schedule, then set the schedule's options. You do not have to set a schedule for the script; you might prefer not to, if this utility script will only need to be run occasionally, you can execute it manually by clicking the Run button in the toolbar.
9. Click the Options tab, then set the script options you desire. See "Copy Backup Script Options" for more information.

Copy Backup Script Options

All of the options for this kind of script are found in other script types. See "Backup script Options" or "Copy Media Set Options," earlier in this chapter. The default options for Copy Backup scripts are "Media verification," "Match Source Media Set to destination Media Set," and "Don't add duplicates to the Media Set."



Creating a Verify Script

A Verify script allows you to specify a Media Set and run a verification on it, ensuring that the files and folders in the Media Set correspond to the files and folders on the Sources.

Verification scripts provide the ability to schedule Media Set media verification. This "offline verification" is a useful tool for maximizing your backup window. 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 Media Set media by comparing the files in the source Media 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 any backups that took place when Retrospect's "Generate MD5 digests during backup operations" preference was disabled. In these cases, Retrospect still checks all files on the Media

Set media to make sure that they are at least readable, but without the MD5 digests, Retrospect cannot determine the integrity of these files.

Note: *Verification scripts do require you to reinsert media when verifying backups that span media.*

To create a Verify script, follow these steps:

1. In the Retrospect console's Sidebar, click Scripts.
2. In the List View Toolbar, click the Add button. The Script dialog appears.
3. In the Script Name field, enter a name for your new Verifying script.
4. Make sure that the Utility category is selected, then click Verifying in the script types list on the right side of the dialog, then click Add. The new script appears in the list, with a red icon next to it, indicating that the script is not complete. Below, in the Details area of the Summary tab, you can see that it is blank, telling you that you need to specify the Media Set(s) you wish to verify, and if necessary, to schedule the script.
5. Click the Media Sets tab. From the list of Media Sets, choose one or more by clicking the checkboxes next to them.
6. Click the Schedule tab. If you want the Verify script to execute at some regular interval, click the Plus (+) button to create a schedule, then set the schedule's options. You do not have to set a schedule for the script; you might prefer not to, if this utility script will only need to be run occasionally, you can execute it manually by clicking the Run button in the toolbar.
7. Click the Options tab, then set the script options you desire. See "Verify Script Options" for more information.

Verify Script Options

There are only two options available for Verify scripts, both of which are off by default:

Verify entire Media Set: By default, Verify scripts only verify data not previously verified using the verify script. Use this option to force verification of the entire Media Set with each execution of the script.

Eject tapes and disks 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.

Creating a Groom Script

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 Media 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. Groom scripts have no options.

To create a Groom script, follow these steps:

1. In the Retrospect console's Sidebar, click Scripts.
2. In the List View Toolbar, click the Add button. The Script dialog appears.
3. In the Script Name field, enter a name for your new Groom script.
4. Make sure that the Utility category is selected, then click Groom in the script types list on the right side of the dialog, then click Add. The new script appears in the list, with a red icon next to it, indicating that the script is not complete. Below, in the Details area of the Summary tab, you can see that it is blank, telling you that you need to specify the Media Set(s) you wish to groom, and if necessary, to schedule the script.
5. Click the Media Sets tab. From the list of Media Sets, choose one or more by clicking the checkboxes next to them.
6. Click the Schedule tab. If you want the Groom script to execute at some regular interval, click the Plus (+) button to create a schedule, then set the schedule's options. You do not have to set a schedule for the script; you might prefer not to, if this utility script will only need to be run occasionally, you can execute it manually by clicking the Run button in the toolbar.

Duplicating Scripts

You don't always have to create a script from scratch. If you already have a script that is similar to the one you want to create, simply duplicate that script, then modify it as necessary.

To duplicate a script, follow these steps:

1. In the Retrospect console's Sidebar, click Scripts.
2. In the list of scripts, click to select the one you want to duplicate.
3. In the toolbar, click the Duplicate button. Retrospect asks you to name the new script, and gives you a default name of "script name Copy." Enter a name for the new script and click Duplicate. The new script appears in the scripts list.
4. Click on each of the tabs in the script's detail area and make the changes that you desire.

Chapter 6: Disaster Recovery

By definition, a disaster is when something really bad happens. Part of your backup strategy needs to plan for disaster in order to accomplish the recovery of your data in its aftermath. That's what this chapter is about. The disaster can be as simple as a hard drive failure or computer theft, or be the result of a physical disaster, such as a fire or a flood.

Overview of Disaster Recovery

The key principle behind disaster recovery is simple, yet critical: if you don't back up everything, you can't restore everything. That's why, as part of your overall backup plan, you must include complete backups of each computer you want to protect, not just the contents of a Favorite Folder. You'll then use the contents of a complete backup to restore all of your data.

When you need to recover from a disaster, you often don't have the ability to boot from the computer that will be the destination for the restore. For example, if the computer's hard drive had failed, but the replacement typically gets installed with no operating system present. Retrospect can do this sort of "bare metal" recovery in more than one fashion, depending on how you performed your backups.

Preparing for Disaster Recovery

Retrospect offers two different types of backup. The first is the traditional archival method, called a *backup*, where Retrospect adds new and changed files to one or more of its Media Sets, essentially building an archive of every file that Retrospect has seen. This method saves both deleted files and previous versions of files, and it allows recovery to any backed up point in time. The Retrospect application must be used to perform restores from a backup.

The second method of backup is a clone-like operation, called a *copy*, where Retrospect makes a target disk look like the source disk by copying files and folders—in their native format—over to the target. This method has the advantage of providing a bootable copy of the source disk (as long as the original contained a bootable operating system), and it also has an option to save files in the copy that were deleted from the source. However, this method has the drawback of not keeping older versions of files, and for the copy to be bootable, each disk so protected needs its own target disk.

Procedures for performing backup and copy operations are found in Chapter 5, "Working with Retrospect."

Whether you have protected your data with a backup or a copy, the basic procedure is similar: you will be starting up the computer to which you will be

restoring data (we'll call that the target) with another Mac or an external hard drive (we'll call that the source).

The options for disaster and bare metal recovery that follow all assume that you now have a Mac with a functioning hard disk that needs to be completely restored from a backup or copy (i.e., any damaged, failed, or missing hardware has been replaced or repaired).

Taking care of your Catalogs

Each Retrospect Media Set has a corresponding Catalog—a database, really—that tells Retrospect exactly which files are contained in the Media Set, where they are on the media, and other information. To be able to restore from a Media Set, Retrospect needs to be able to access the Catalog belonging to that Media Set. If you no longer have the Catalog file, then you will need to rebuild it first by clicking the Rebuild button in Retrospect's Media Sets view. Rebuilding a Media Set's Catalog can take a long time, because Retrospect has to scan the media and read every file.

By default, Retrospect stores Catalog files on the Retrospect server in `/Library/Application Support/Retrospect/Catalogs/`. It's a good idea to periodically copy your Catalogs to alternate storage media, such as separate hard disk, a writable DVD, a flash drive, or another computer on the network.

Detailed instructions for safeguarding your Catalog files can be found in Chapter 7, under "Catalog and Configuration Backups." In the same chapter, you can find instructions for rebuilding Catalogs, under "Rebuilding a Media Set."

Creating a Mac OS Emergency Tools disk

It can be very helpful, and save you a lot of time, if you prepare for disaster recovery by creating an Emergency Tools external hard disk that you can use to boot machines that you want to restore. This disk should contain the following:

- Mac OS X (so that it is bootable)

- The Retrospect console application and engine if you will want to recover the Retrospect backup server
- An installed copy of the Mac Retrospect Client, so that you can use the Emergency Tools disk to restore data from the Retrospect server over the network
- The Retrospect Client installation folder, containing the Client software for Macs, Windows, and Linux machines, as well as copies of any public/private keys in use by your Retrospect installation
- Other utility software that you find useful, such as Micromat's TechTool Pro and Alsoft's Disk Warrior

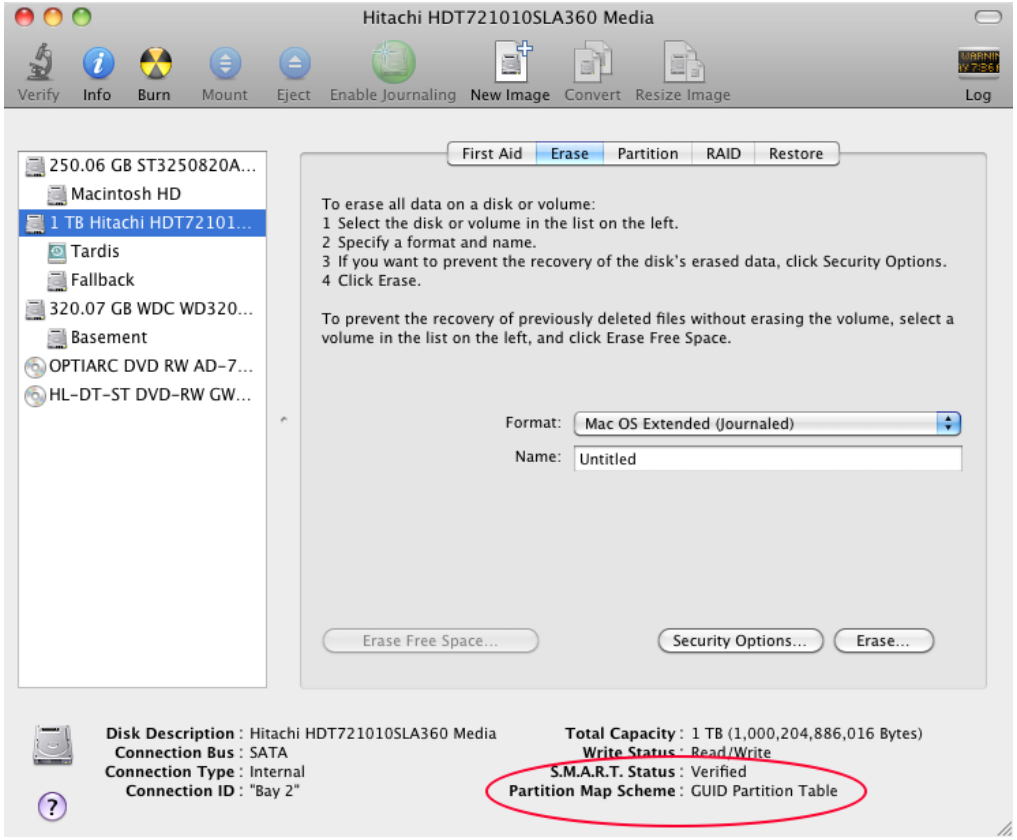
USB or FireWire?

When you build your Emergency Tools disk, you need to decide whether you are going to use an external disk drive that is connected using USB or FireWire (though some drives have both). Either connection method can work. Remember that Apple has made some Intel-based machines that lack FireWire altogether, so a USB-connected drive may be a better choice. However, you'll have to make the final determination based on the mix of Mac models in your organization.

Noting disk partitioning schemes

It's easy to start up a Mac from an external hard drive, but it's important to remember a few key points. Intel Macs and PowerPC Macs require different disk partition schemes, so a disk made to start up an Intel Mac won't start up a PowerPC Mac, and the opposite is also true. Intel-based Macs can only be booted with disks that use the GUID Partition Table scheme; PowerPC-based Macs can only be booted with disks that use the Apple Partition Map scheme.

This means that you'll need to be sure of the disk partitioning scheme used on any disk from which you hope to start up your Mac. You can check which partitioning format is used by running Apple's Disk Utility application, selecting the hard disk you want to check, and noting the portioning scheme shown. Just be aware that repartitioning a disk to change its partition scheme will erase all the data already present on that disk.



If you prepare an Emergency Tools hard drive, and you have both Intel Macs and PowerPC Macs on your network, you'll really need to create two Emergency Tools hard drives, one formatted for Intel Macs, the other for PowerPC Macs.

Intel-based Macs support starting from an external USB storage device that contains an installation of Mac OS X 10.4.5 or later, which is compatible with the Mac that the USB device is connected to. Don't use a version of Mac OS X that is older than the version of the Mac you want to restore shipped with. And remember that the Retrospect console application requires Mac OS X 10.5.5 or later (though the Retrospect Client and engine can run on Mac OS X 10.4.11 and later).

Note: *Since Mac OS 10.6 (Snow Leopard) dropped support for PowerPC based Macs, you can't use it to boot those machines. We suggest that you install Mac OS X 10.5.8 (Leopard) as the operating system on your Emergency Tools disk.*

Restoring a Mac from Regular Backups

If you had previously backed up the target Mac using Retrospect's backup method, the backed-up data will be contained within a Media Set, and you'll need to use Retrospect to do the restore.

Using FireWire Target Disk Mode

Macs with FireWire ports have a special hardware feature that can aid in disaster recovery, called Target Disk Mode. This feature allows you to turn a Mac (in this case, the Mac to which you wish to restore data) into an external hard disk drive that can be connected via FireWire to another Mac (ideally, the Retrospect server, because you will get the fastest restores over FireWire, rather than over the network). Target Disk Mode works with either FireWire 400 or FireWire 800 ports (naturally, data transfer will be faster over FireWire 800).

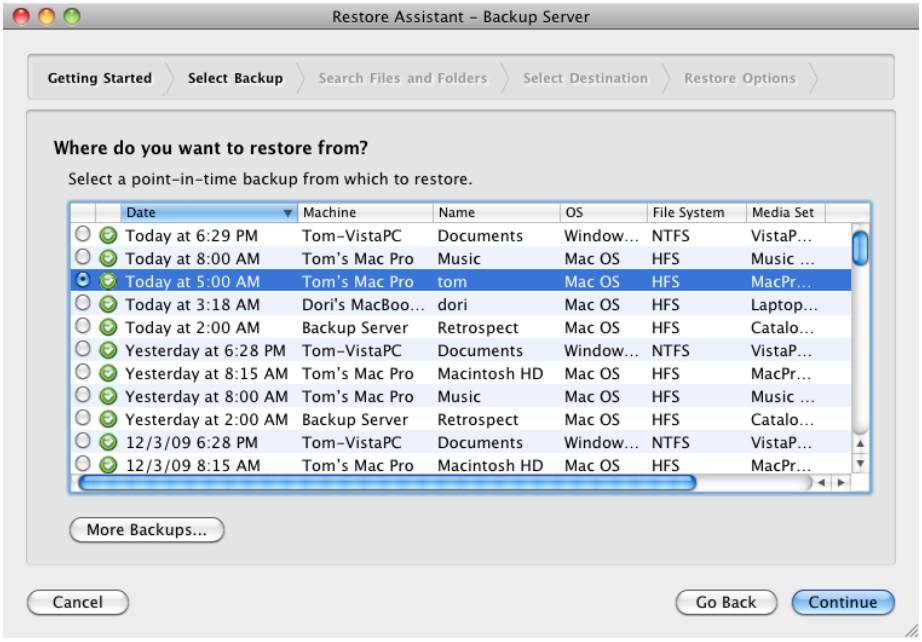
To perform a restore using FireWire Target Disk Mode, follow these steps:

1. To start the target Mac (the one to which you wish to restore data) in Target Disk Mode, turn it on and immediately hold down the T key on the keyboard. When the FireWire symbol appears and bounces around the screen, you can release the T key; the Mac is now in Target Disk Mode and can be connected to any other Mac with a FireWire cable.
2. Make sure the source Mac (which needs to have the Retrospect engine installed) is turned on, then connect the FireWire cable from the target Mac to the source Mac. The hard disk of the target Mac will appear on the source Mac's desktop, as if it were any other external drive.
3. In the Finder on the source Mac, Get Info on the target Mac's volume you want to restore and ensure that the "Ignore ownership on this vol-

ume" option is unchecked. Otherwise, Retrospect will not be able to restore file and folder permissions properly on the target disk.

4. Start the Retrospect console.
5. (Optional) If your Catalog files are not available, rebuild the necessary Catalog from your backup media. See "Rebuilding a Media Set," in Chapter 7, for detailed instructions. If you copied your Catalog files from backups, you must get Retrospect to recognize them. From the Media Sets category, click Locate, navigate to the location of the Catalog file, and click OK to add the catalog to the list of available Media Sets.
6. In the Retrospect toolbar, click Restore. The Restore Assistant window appears.

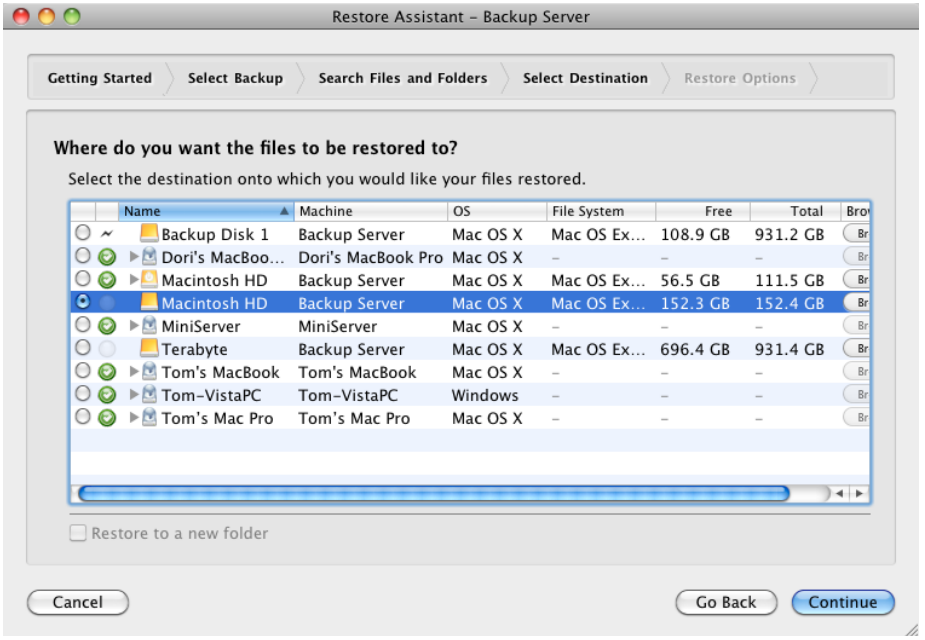
7. Choose "Restore an entire source volume or favorite folder to a previous point in time," then click Continue. The Select Backup pane appears.



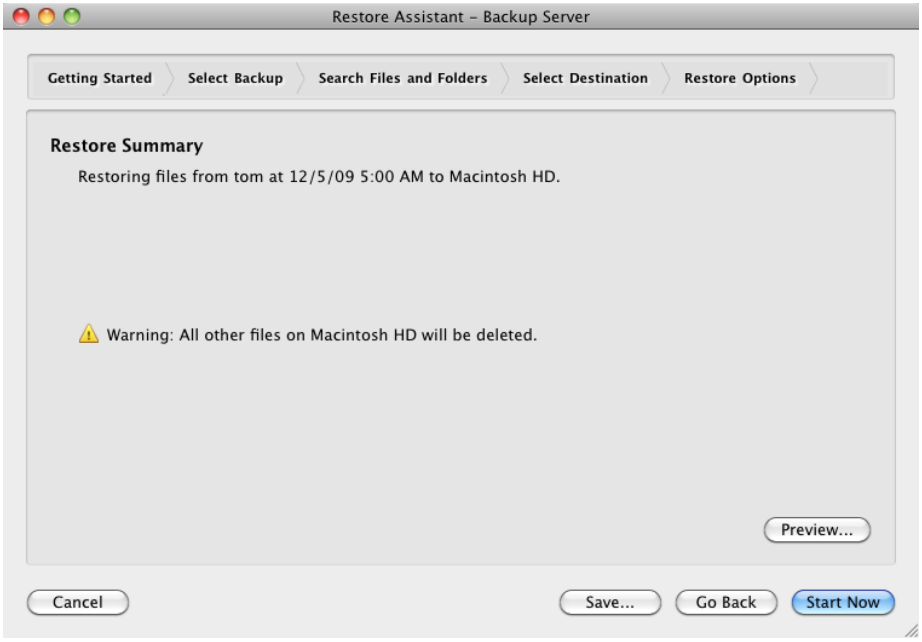
8. Choose the backup that reflects the point in time to which you want to restore.

   Note: *In the list, it's possible that the point in time you chose will show only the files that were backed up during that particular backup run, leading you to think that only those files will be restored. However, because of the choice you made in Step 7, all of the files on the source volume will be restored, as you want.*

   If you have many backups, you may find it easier to sort the list by Machine or Media Set. Click the heading of the column by which you want to sort. Click the heading again to reverse the sort order. When you have found and selected the backup you want, click Continue. The Select Destination pane appears.



9. Click the radio button next to the name of the destination volume, then click Continue. The Restore Options pane appears, recapping the source and destination of the copy.



10. When you are ready to perform the restore, click Start Now.
11. When the restore is complete, eject the Target Disk Mode Mac's disk and start it up normally.

Restoring a Mac client using an Emergency Tools disk

In this method of disaster recovery, you will start up the target Mac using your previously prepared Emergency Tools hard drive and restore it as a Retrospect client computer. Follow these steps:

1. Connect your Emergency Tools hard drive to the target Mac. Turn it on, then start the target Mac. Since the target Mac should not have an operating system, the Mac should find and boot from the Emergency Tools hard drive. If necessary, hold down the Option key on the keyboard to choose which disk will be used as the startup disk.
2. On the Retrospect server, log in the client to be restored.
3. In the Retrospect toolbar, click Restore. The Restore Assistant window appears.

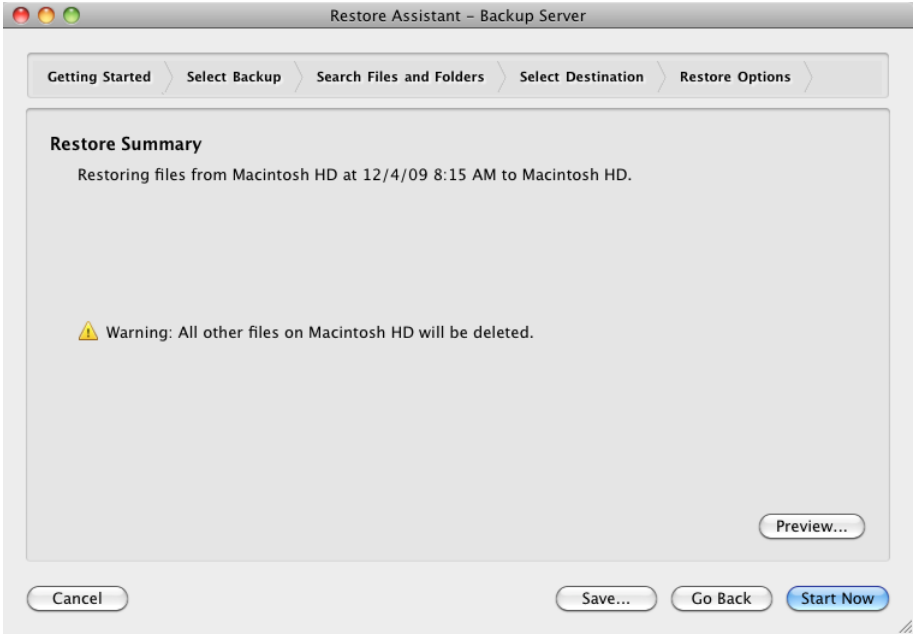
4. Choose "Restore an entire source volume or favorite folder to a previous point in time," then click Continue. The Select Backup pane appears.
5. Look through the list of backups until you find the backup that reflects the point in time to which you want to restore. When you have found and selected the backup you want, click Continue. The Select Destination pane appears.
6. Click the radio button next to the name of the destination volume on the client to be restored, then click Continue. The Restore Options pane appears, recapping the source and destination of the copy.
7. When you are ready to perform the restore, click Start Now.
8. When the restore is complete, shut down the Mac by choosing Shut Down from the Apple menu.
9. Disconnect the Emergency Tools disk, then start the restored target Mac normally.

Doing a live restore

A **live restore** is any time you restore over a Mac's current, in-use startup disk. It is used any time that you need to restore a functioning Mac to a previous point in time, and also when you don't have a second computer or an Emergency Tools startup disk to help perform the restore. Follow these steps:

1. If the Mac won't boot, tnstall Mac OS X on the target Mac. The version of the operating system must be the same as the version on the backed-up data. If you are forced to install a later version of Mac OS X, see the instructions under "What to do if the OS on the new Mac is newer than the backed-up OS," later in this chapter.
2. Install the Retrospect Client software on the target Mac.
3. On the Retrospect server, log in the client to be restored.
4. In the Retrospect toolbar, click Restore. The Restore Assistant window appears.

5. Choose “Restore an entire source volume or favorite folder to a previous point in time,” then click Continue. The Select Backup pane appears.
6. Look through the list of backups until you find the backup that reflects the point in time to which you want to restore (usually the latest backup). When you have found and selected the backup you want, click Continue. The Select Destination pane appears.
7. Click the radio button next to the name of the destination volume, which is the startup volume of the target Mac client, then click Continue. The Restore Options pane appears, recapping the source and destination of the copy. Note that the warning message is different (“Warning: All other files on disk name will be deleted.”), indicating that if there are any newer files on the disk than those contained in the backup, those newer files will be deleted.



8. When you are ready to perform the restore, click Start Now.

9. When the restore is complete, restart the Mac by choosing Restart from the Apple menu. Upon restart, the Mac will be in the restored state.

Restoring a Mac from a Copy

If you have been using Retrospect's Copy operation, disaster recovery can be quite simple. By definition, a Copy script creates an exact copy of all the files on the source disk onto another hard disk, so that disk is bootable. By starting up the replacement Mac from the disk that contains the copy, you can get back to work immediately; the only drawback, as with any backup, is that files created or changed since the last time the copy was made will remain unavailable.

Start up and restore from the copy

Most of the time, you will be performing Copy operations onto single external hard drives (though it is certainly possible to use more exotic hardware setups, such as enclosures with multiple drives). To restore to the internal drive of the repaired Mac, follow these steps:

1. Connect the hard drive containing the copy to the Mac you want to boot and restore.
2. Turn on the external drive and then turn on the Mac. If the Mac has an operating system installed, hold down the Option key as you turn it on. This will launch the Startup Manager and display the available volumes from which you can start up.
3. Use the left and right arrow keys on the keyboard to select the volume you would like to use, in this case the external drive containing the copy backup.
4. Press the Return key on your keyboard to start the computer from the volume you selected.
5. Once the startup process is complete, you may use the computer while booted from the backup disk.

6. Use Retrospect's Copy Assistant to copy the backup disk's contents back to the internal drive, replacing any files that might be on the internal drive. See "Using the Copy Assistant" in Chapter 5 if you need detailed instructions.

Restore from the copy, followed by a live restore

You may be faced with a situation where you have multiple backups of the Mac that needs disaster recovery: a fairly recent copy, and an even more recent regular backup. In this case, you would ideally want to use the copy to restore the target Mac quickly, then you want to use the newer files in the regular backup to restore the latest versions of files, applications, and user settings.

To accomplish this kind of restore, follow the steps earlier in this chapter, first under "Start up and restore from the copy," then under "Doing a live restore."

What to do if the OS on the new Mac is newer than the backed-up OS

In some situations, you may be required to restore to a target Mac that must use a newer version of Mac OS X than the old Mac that was backed up. For example, the old Mac could be an older MacBook that was running Mac OS X 10.4 ("Tiger") and was stolen. The newly-purchased replacement MacBook came with Mac OS X 10.6 ("Snow Leopard") and because of hardware changes, can't run the older operating system, so you can't simply perform a restore onto the newer hardware.

In this case, you have two options:

1. Restore the most recent backup of the old Mac to an external hard disk drive, and then use the new Mac's Migration Assistant application to copy the apps and user data over from the external drive. (The best results will be achieved with this method.)
2. Use Retrospect's "Restore selected files and folders" option to hand-pick items for restore (this method is tedious, so it's better to buy an

external hard disk drive and proceed with method #1). If you need information on restoring selected files and folders, see "Using the Restore Assistant to Find and Restore Files and Folders" in Chapter 5.

Restoring a Windows Client

The following instructions describe how to restore an entire volume on a Windows client over the network. These instructions assume that you have a newly erased disk that has had installed a fresh copy of the same version of Windows that was previously on the backed-up machine.

You must first get the client computer operating with the network before performing the actual restore operation from the backup computer.

The steps below involve completely replacing the contents of a client computer's hard drive with a previous backup in which you backed up "all files."

1. Install new Windows system software on the newly-formatted hard disk. Restart from this volume.
2. Use the Setup program to install the Retrospect client software as described in "Installing Retrospect Client software on a machine running Microsoft Windows" in Chapter 1.
3. From the Sources category of the Retrospect console, Remove the old client, then Add the new client.
4. In the Retrospect toolbar, click Restore. The Restore Assistant window appears.
5. Choose "Restore an entire source volume or favorite folder to a previous point in time," then click Continue. The Select Backup pane appears.
6. Look through the list of backups until you find the backup that reflects the point in time to which you want to restore. When you have found and selected the backup you want, click Continue. The Select Destination pane appears.

7. Click the radio button next to the name of the destination volume, then click Continue. The Restore Options pane appears, recapping the source and destination of the copy.
8. When you are ready to perform the restore, click Start Now.
9. Restart the client computer.
10. 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 Linux Client

The following instructions describe how to restore an entire volume on a Linux client over the network. These instructions assume that you have a newly erased disk that has had installed a fresh copy of the Linux operating system distribution.

You must first get the client computer operating with the network before performing the actual restore operation from the backup computer.

The steps below involve completely replacing the contents of a client computer's hard drive with a previous backup in which you backed up "all files."

1. Install new Linux 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.
2. Use the Setup program to install the Retrospect client software as described in "Installing Retrospect Client software on a machine running Linux" in Chapter 1.
3. From the Sources category of the Retrospect console, Remove the old Linux client, then Add the new client.
4. In the Retrospect toolbar, click Restore. The Restore Assistant window appears.
5. Choose "Restore an entire source volume or favorite folder to a previous point in time," then click Continue. The Select Backup pane appears.

6. Look through the list of backups until you find the backup that reflects the point in time to which you want to restore. When you have found and selected the backup you want, click Continue. The Select Destination pane appears.
7. Click the radio button next to the name of the destination volume, then click Continue. The Restore Options pane appears, recapping the source and destination of the copy.
8. When you are ready to perform the restore, click Start Now.
9. Restart the client computer.

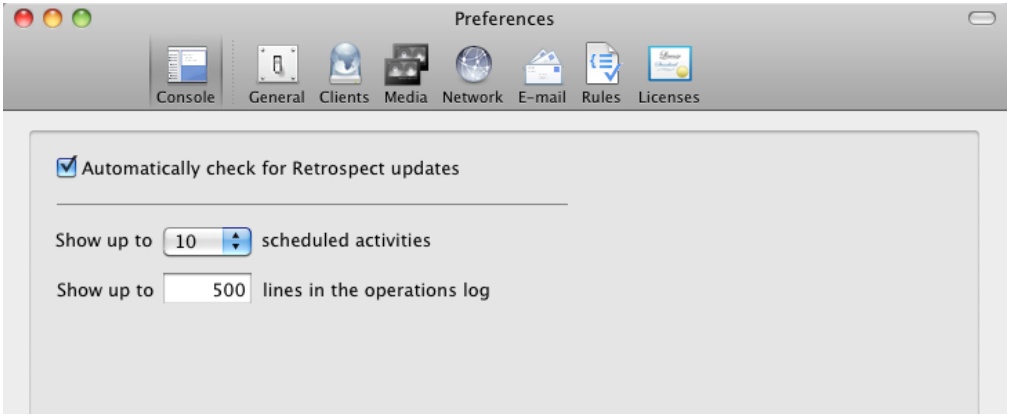
Chapter 7: Managing Retrospect

This chapter describes how to use several aspects of Retrospect, such as its Preferences, in detail, and how to perform various tasks, such as managing media sets, viewing reports, and maintaining scripts. It also offers advice on using Retrospect to perform more effective backups.

Retrospect Preferences

You can adjust Retrospect preferences to modify the program's behavior to best meet your needs. Retrospect preferences affect all operations performed by Retrospect.

Open the Preferences window by choosing Preferences from the Retrospect menu. The Preference window appears, with a toolbar that allows you to display each section of the application's preferences. Click on the icon in the toolbar to display that section of Preferences. Retrospect remembers the last preference panel you previously worked with, so when the window appears, it is already set to that panel.



Console Preferences

The Console preferences apply to the Retrospect console, and apply across all Retrospect engines you may have logged in.

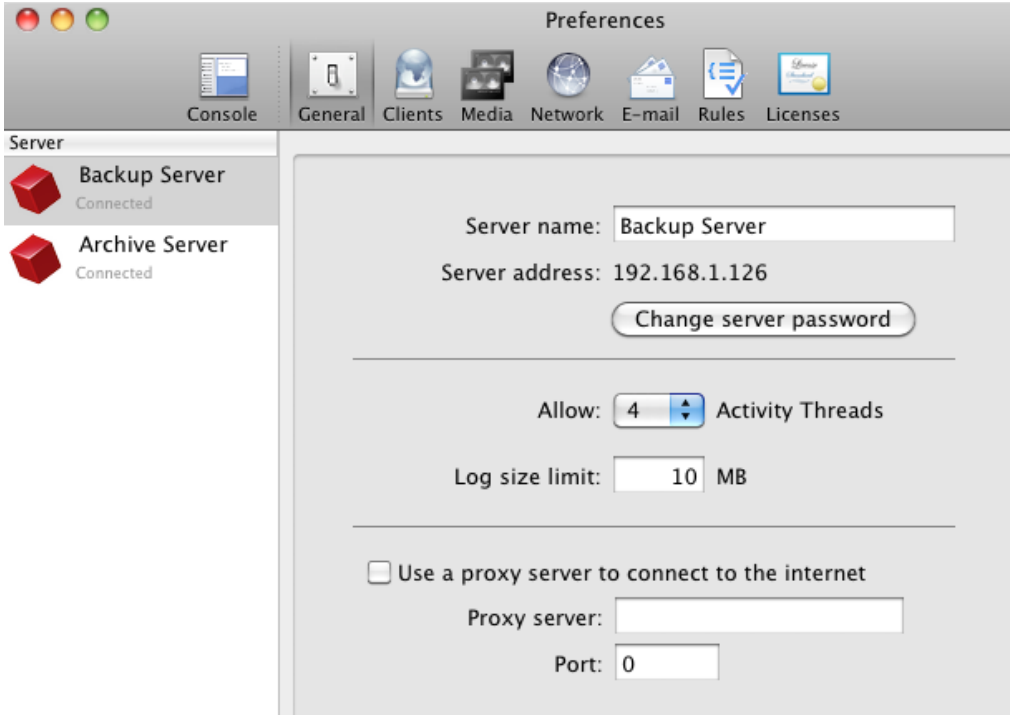
Automatically check for Retrospect updates tells Retrospect to check for updates to the program when you launch the console.

Show up to *n* scheduled activities controls the number of upcoming activities that appears in the console, under the Activities category. In the pop-up menu, you can choose from 10, 20, 50, or 100 activities to be shown. This is needed as a script set to back up every day would have 365 scheduled activities just for one year.

Show up to *n* lines in the operations log allows the operations log to fill up to the specified number of lines. When the log reaches the limit set, the oldest entries are no longer shown, though they remain in the `operations_log.utx` file stored in `/Library/Application Support/Retrospect/`, up to the maximum log size specified in General Preferences (see "Log size limit" below). You can view the operations log by choosing View > Log, or by pressing Cmd-L. Type the length you want for the log in the entry field.

General Preferences

In General preferences, you set preferences for each logged-in Retrospect server. Each server you have logged in appears in the list on the left of the window. Click on the server you want to control in the list.



Server name can be anything you want; simply type in the field to change it. By default, Retrospect uses the server machine's Computer Name as shown in System Preferences' Sharing panel as the server name, but you may change it

to be more descriptive to you and your users. The Server name is displayed to your users in the History section of the Retrospect Client among other places.

Server address is the IP address of the server computer. This field cannot be changed after the server has been logged in.

Change server password allows you to assign a password for access to the selected server. Clicking the button presents a dialog where you can enter the old password (if any), enter a new password, and then enter the new password again to confirm. Click the Change password button to accept the change.

Allow *n* Activity Threads provides a pop-up menu with numbers from 1 to 8. Setting the number of activity threads tells Retrospect how many simultaneous activities, such as multiple backup and restore operations, it can run at the same time. By default, a Retrospect engine is set for four concurrent activity threads. The number of activity threads that can be run at any one time efficiently is a function of the hardware capabilities of the Retrospect server machine as well as the type of task the thread will handle. Factors include the speed of the machine's processor and the amount of its installed RAM but also the number of files being transferred. In general, you should have one Gigabyte of free RAM for each activity thread you will run.

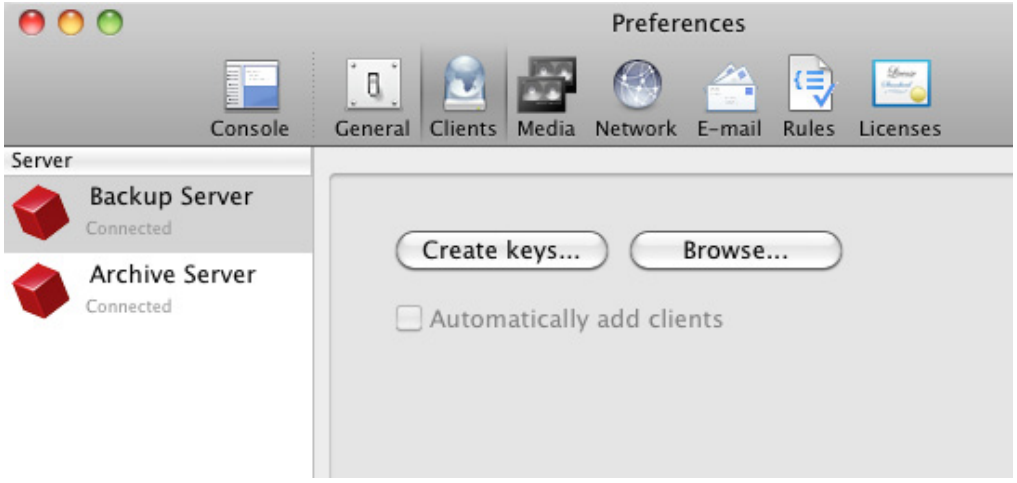
Log size limit allows you to set a number, in megabytes, for the size of the Operations Log. The default setting is 10 MB. When the log reaches the limit, the oldest portion of the log is deleted to keep its size within the limit. The bigger the log is, the longer it will take to open. Type the maximum size of the Operations Log in the entry field.

Use a proxy server to connect to the Internet allows you to set up another computer as an intermediary between the Retrospect server and the Internet when sending email notifications. The Retrospect server will connect to the proxy server, which will interpret the Retrospect server's request and pass it on to the Internet according to whatever filtering rules set for the proxy server. Click the check box to activate this feature, then enter the IP address or DNS name in the Proxy server entry field, and if necessary enter the port number the proxy server will be listening on.

Clients Preferences

Public/Private Key Authentication is a method by which Retrospect Clients can be logged into a Retrospect server automatically through use of matching encryption key sets. In the Clients pane, you can create these AES-256 encrypted private and public key certificate files for your Retrospect Clients.

To set up this authentication, you will create two files, which are created on the Retrospect Server at `/Library/Application Support/Retrospect/`. The private and public key files are named `privkey.dat`, and `pubkey.dat`, respectively. The `privkey.dat` file remains on the Retrospect server, and the `pubkey.dat` file is copied to each of the Retrospect Clients.



To create the keypairs and install them with your Retrospect Clients, follow these steps:

1. In Preferences > Clients, click “Create keys...”, enter a password of eight characters or more for key creation, then click Create. Retrospect may take up to a minute or more to generate the keys, depending on the speed of the computer.
2. If you want Retrospect to automatically log in clients with the proper public key, check “Automatically add clients”. This is recommended.

3. From the Retrospect Installer disk image or CD, open the Client Installers folder, then copy the Mac Client Installer folder onto your hard drive.
4. In the Finder, locate the pubkey.dat file in `/Library/Application Support/Retrospect/` and copy it into the folder named "public_key" inside the Mac Client Installer folder on your hard drive.
5. Distribute or copy this public_key folder containing the pubkey.dat file along with the Retrospect Client installer.
6. After installing the Retrospect Client software on each computer, they can be logged in (or will be automatically logged in, if that option was set) at the Retrospect server.

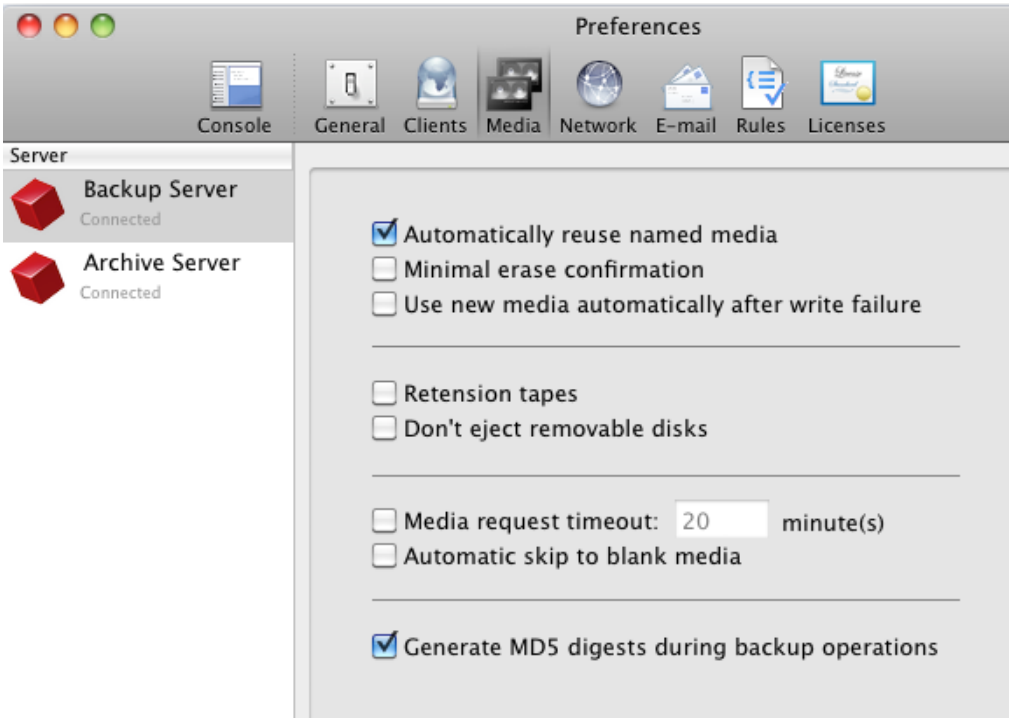
If keypair files already exist on the Retrospect server, you may load them by clicking the Browse button, then navigating to the folder that contains the two keypair files, then clicking Select. This can be used to share the same keypair files between multiple Retrospect backup engines.

Media Preferences

Media preferences controls how Retrospect works with media such as tapes, hard disks, and other media.

Automatically reuse named media tells Retrospect not to confirm with the user the erasure of media that has the same name that already contains data. For example, if you have one or more tapes that are part of a Media Set named Tape Backup A, and a script is set to automatically recycle the Media Set's members at a regular interval, unchecking this box will cause Retrospect to require confirmation before erasing each member of the Media Set.

Minimal erase confirmation, when checked, 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 media set named "1-Media 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.

Use new media automatically after write failure tells Retrospect to skip to blank media when it encounters a failure to write to the media, rather than reporting a failure and canceling the activity.

Retension tapes is used with older tape drives such as Travan, OnStream, and DC 6000 drives. It tells Retrospect to automatically wind the tape forward to the end and rewind after the script finishes to even out the tension and alignment.

Don't eject removable disks. By default, Retrospect will automatically eject removable disks after a script finishes. Checking this prevents this from happening.

Media request timeout: *n* minutes sets the amount of time that Retrospect will wait for media to become available during execution. For example, if you're using a tape autoloader, it may take several minutes for the device to find and load a particular tape in the Media Set. This preference is off by default, so media requests never time out.

Automatic skip to blank media uses a blank tape or disk when the last member of the Media Set is not available, even if that last member is not yet full.

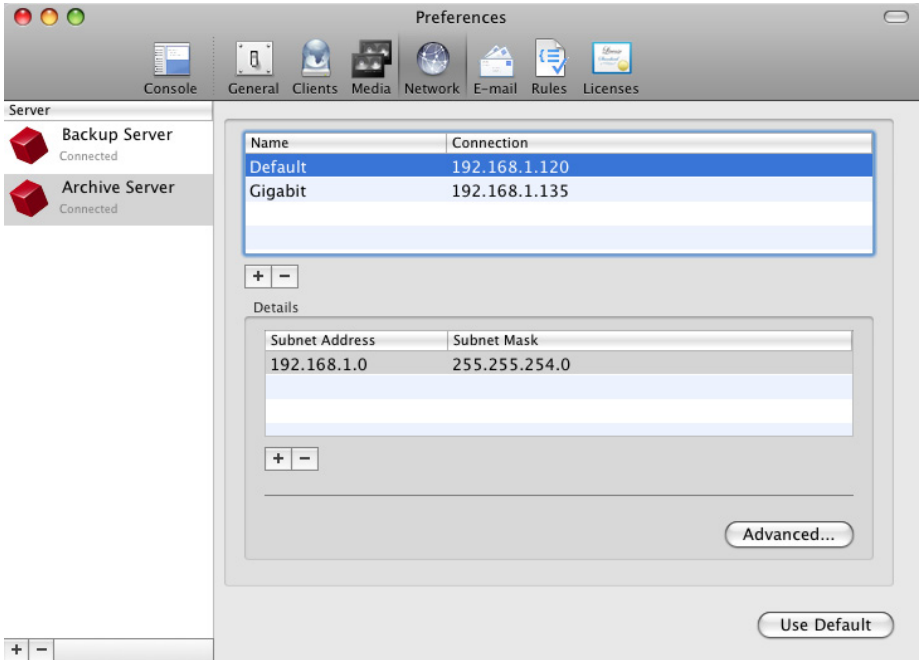
Generate MD5 digests during backup operations is on by default. It tells Retrospect to create MD5 hash digests as part of backup operations. Retrospect later uses these digests to speed up media verification.

Network Preferences

Out of the box, Retrospect is able to back up clients without any additional configuration. If your backup computer has multiple network interfaces or your clients are in different subnets, Network preferences allows you to manage how Retrospect accesses these backup clients. For example, a custom network interface lets you back up clients on different subnets without requiring backup data to cross routers, conserving network bandwidth.

You can name and assign different network interfaces to specific network addresses in Retrospect's preferences, which will use the addresses in order. To do this, follow these steps:

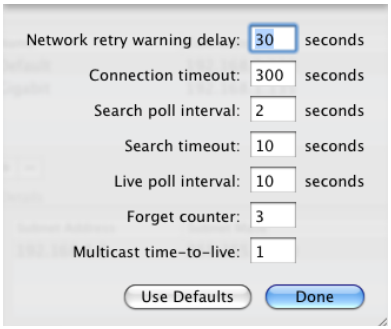
1. Choose Retrospect > Preferences > Network. If more than one Retrospect server appears in the Server column, select the server you want to control. In the connection list on the right side of the window, your Mac's default network connect will appear.
2. To add another network interface, click the Plus (+) button below the connection list. In the resulting dialog, choose from the Connection pop-up menu the IP address of the network interface you want to use, then enter a name for the connection and click Add



3. The new connection appears in the connection list. You can also restrict the subnets that Retrospect will use when it looks for clients and network shares. To do that, select one of the connections in the connection list, then click the Plus (+) button below the Details box. In the resulting dialog, enter the Subnet Address and Subnet Mask, then click Add. The subnet restriction will appear in the Details box.

Advanced Settings

Expert users may need additional control over Retrospect's network behavior. Clicking the Advanced button in the Network preference pane brings up a dialog with the following settings:



Connection timeout The maximum amount of time Retrospect will wait for a client before logging an error and going to the next activity. Set this to a higher value if you receive -519 (network communication failed) errors and you know your network is slow.

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.

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.

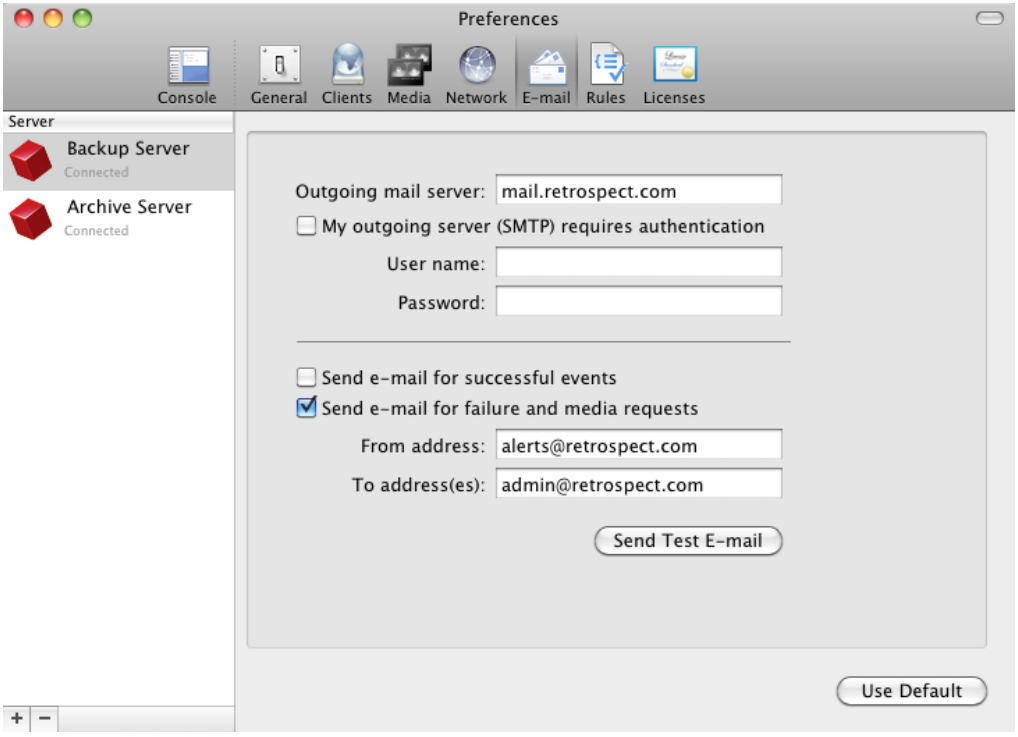
Multicast time-to-live Retrospect assigns this "time to live" number to multicast UDP packets. It is the maximum number of router hops a packet can make before it is discarded. An increase in the time to live number lets Retrospect search for clients on more subnets connected by IGMP capable routers. Routers which do not support IGMP will not forward the multicast UDP packets.

Enter a value next to the settings you want to change, then click Done.

Warning: Make changes in this dialog only if you know exactly what you're doing, or at the direction of Retrospect tech support. Under some circumstances, changes in this dialog can adversely affect Retrospect performance. Be careful! If you make a mistake, but are unsure what change caused problems, you can revert *all* of Retrospect's preference settings for the selected server by clicking the Use Default button.

Email Preferences

Retrospect has the ability to send e-mail notifications for both successful executions and problems. In the E-mail preferences pane, you can set the outgoing mail server that Retrospect should use, and the e-mail addresses that Retrospect will use to send the alerts. By default, Retrospect will not send e-mail alerts.



Outgoing mail server is an entry field where you can enter either a machine name (preferred) for the outgoing mail server or an IP address. You can also specify the TCP/IP port over which Retrospect should communicate with the mail server by appending its address with the port number, [serverIpAddress]:[portNumber], as in this example: `smtp.servername.com:26`.

My outgoing server (SMTP) requires authentication should be checked if the outgoing mail server requires a login.

User name: If the outgoing mail server needs a login, enter the user name assigned to Retrospect by your mail administrator.

Password: If the outgoing mail server needs a login, enter the password assigned to the associated user name.

Send e-mail for successful events should be checked if you want Retrospect to notify you every time it completes a successful execution. Be aware, however, that if you have many scripts running, you may receive a large number of e-mails.

Send e-mail for failure and media requests should be checked if you want Retrospect notify you when there are problems during execution. If you check this option, you will need to enter valid e-mail addresses in the From address and To address(es) entry fields. Note that you may specify multiple recipients in the To address(es) field. Separate each e-mail address with a comma.

Send Test E-Mail Click this button to send a test e-mail to the address or addresses in the To address(es) field.

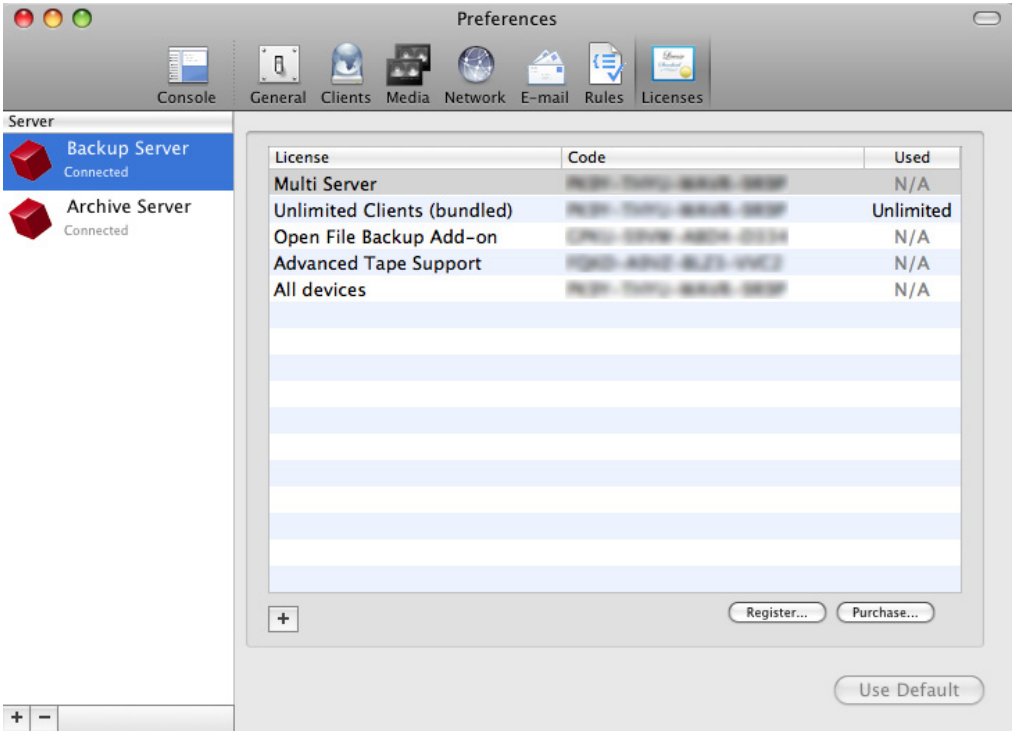
Rules Preferences

The Rules preferences pane allows you to create and manage Rules, which are used to apply conditions to Scripts. See the “Working with Rules” section, on the next page, for more information.

Licenses Preferences

In the Licenses preferences pane, you may enter the license codes you have purchased. Specific license codes unlock specific features of the product, such as Server Client licenses or the Open File Backup add-on for

Windows clients. The first time you connect to a local or remote Retrospect engine, Retrospect opens this preferences pane and asks you to enter your license code for that engine. Enter this information, then click Add.



To enter additional license codes, click the plus (+) button near the bottom of the window. Enter the license code that you have purchased, then click the Add button. The new license code will appear in the window.

To register your Retrospect product online, click the Register button. You'll be taken to a webpage that will walk you through the registration process.

To get information on how to purchase additional Retrospect license codes, click the Purchase button. A dialog will appear with the information.

Working with Rules

You can use Rules with any operation to specify the types of files and folders you want the operation to include. Using Rules to intelligently select or ignore

certain files and folders, you can limit the amount of time and media required for an operation.

Rules let you choose files based on almost any criteria, including name, date, type, or size. Retrospect includes a number of built-in Rules, and you can also create custom Rules. For example, you can create a rule that will choose all Microsoft Word documents modified after August 25, 2009.

A file that is "marked" by a rule (i.e., one that meets the rule's criteria) will not necessarily be copied to the destination. All copying operations (such as backups) using rules are "smart," because of Retrospect's matching feature. For each rule, there is the implied meaning of "select this file, but do not copy it if it already exists in the destination."

You create and modify Rules in the Rules Preferences pane. Choose Retrospect > Preferences, then click the Rules tab.

Retrospect comes with a number of Rules already set up for you. Rules are associated with each server separately, so if you have more than one Retrospect server, you can create different sets of Rules for each server. Simply click on the server in the sidebar of the preference pane to view the Rules for that server.

Tip: *In previous versions of Retrospect, Rules were called Selectors, though the interface used to create them was quite different.*

Using the Built-in Rules

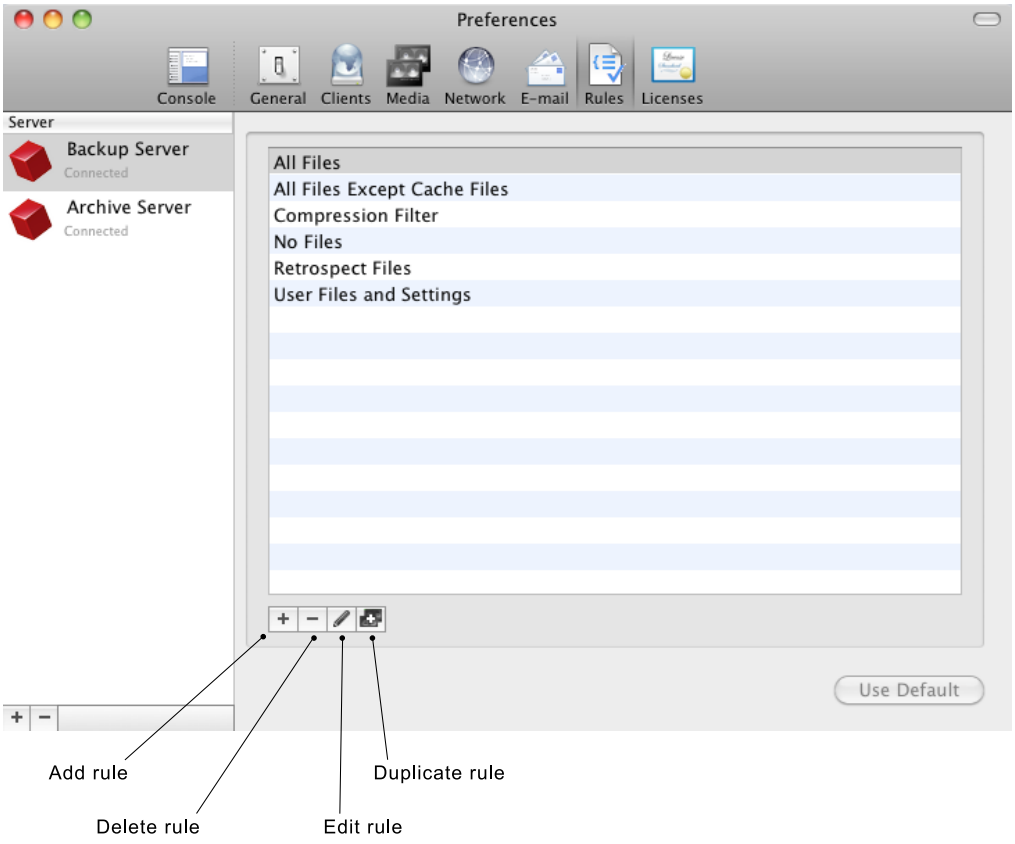
Retrospect includes several built-in Rules, with predefined conditions for selecting files.

Some rules and rule conditions function differently with Mac OS, Windows, and Linux volumes. Examine a rule's details for more information.

Retrospect's built-in Rules are:

All Files marks all files on the source, including the operating system files. This is the default rule.

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 numerous and often large, are not typically useful for restoring.



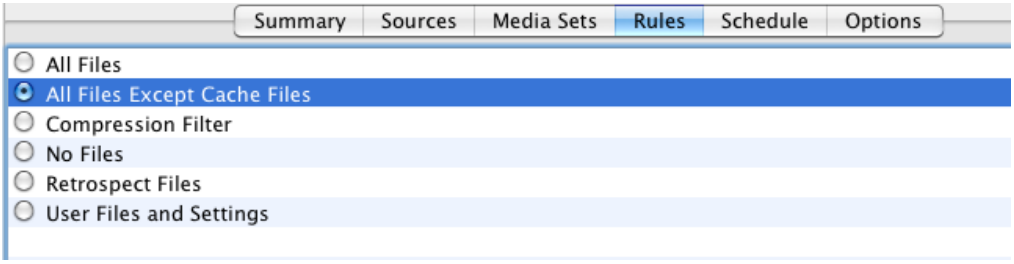
No Files does not mark any files for backup, though Retrospect will still save a complete file and folder listing and associated metadata for each source. Use the No Files rule for testing purposes when you don't want any files copied, or if you want to grab a System State-only backup of a Windows client.

Retrospect Files marks files having the file extensions and some specific file-names used by the Retrospect Backup family.

Users Files and Settings marks files and folders inside the Mac OS X Users, Windows Documents and Settings (in Windows XP, Server 2003), Windows Users (Windows Vista, 7, and Server 2008), and Linux /usr/ folders where users' data and settings are stored.

Applying Rules

You apply Rules during the creation of scripts. One of the steps in creating a script is working with the Rules tab. Click Scripts in the sidebar, select the script you wish to work on in the list, then click the Rules tab below. Select the radio button for the Rule you wish to apply to the script.



Adding or Editing Rules

You may add a Rule, view a Rule, or modify a Rule in the Rules preferences pane. To add a rule, click the Add Rule button, which looks like a plus sign (+) below the list of Rules. To view or edit a rule, select a Rule in the list, then click the Edit Rule button, which looks like a pencil. The Rule dialog appears, showing its three parts:

The **Rule name** can be anything you like. It will appear in the Rules tab of Preferences and Scripts, and will appear in other places within Retrospect.

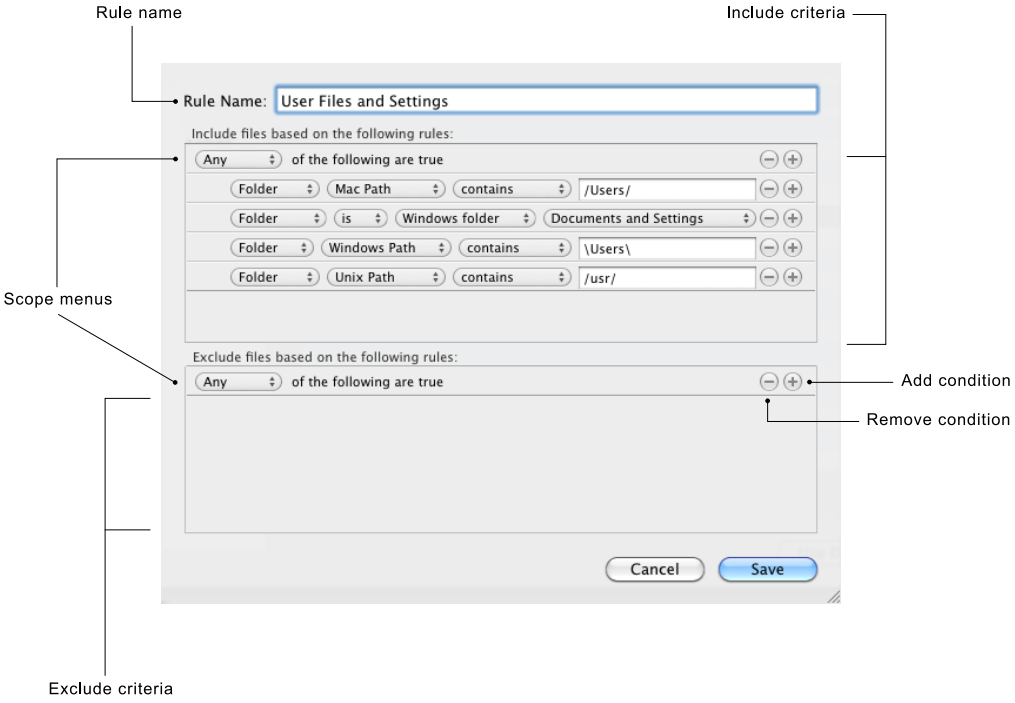
The **include conditions** section is where you tell Retrospect what files and folders you wish the Rule to encompass during the operation.

The **exclude conditions** section is where you tell Retrospect what files and folders to skip during execution.

Each rule must have a Rule name, and then you should add any include or exclude criteria you wish. The default Rule, All Files, has no specific include or exclude criteria, meaning that it includes any file and excludes none.

The scope menus allow you to define the extent of the conditions in either the include or exclude sections. The choices available from the scope menus are All, None, or Any. In the example in the screenshot above, the Any choice in

the include conditions scope menu allows the rule to apply if any of the listed conditions are true, allowing the rule to encompass the user files and settings for Mac, Windows, or Linux clients. In this way, the Any choice acts as a logical *or* condition.

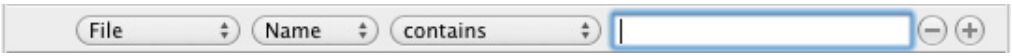


The All choice works as a logical *and* condition. For example, imagine that you want to backup all of the QuickTime movie files that are part of a particular project for your client Widgetco. You've previously saved all the movie files into a single folder. To add the All condition, hold down the Option key on the keyboard. The Add condition plus sign (+) on the "Any of the following are true" scope bar will change to an ellipsis (...), which you can then click to add the All condition. (The None condition is created in the same way, only you can change the All condition to the None condition.) You would then create two conditions:

- Folder Name contains Widgetco
- File Name ends with .mov

The include and exclude conditions sections allow you to add one or more conditions to the rule. You do that by clicking the Add condition button. Similarly, you can delete conditions by clicking the Remove condition button next to an existing condition, and you can also reorder conditions by dragging them on the screen (though it is not possible to drag conditions between the Include and Exclude criteria sections). Rules can have any number of conditions.

After you have added a condition, you need to build it using the pop-up menus and, optionally, the entry field in the condition.



The pop-up menus and entry field are contextual, meaning that whether or not they appear and their contents change depending on the values of other elements within the condition. For example, the first and second pop-up menus interact in the fashion shown on the next page:

The third pop-up menu changes depending on the choices made in the first two menus. For conditions that will also require user input in the entry field, the choices in this third menu narrow the scope of the entry. For example, if you have chosen File in the first menu, and Name in the second menu, the third menu provides the choices **contains, begins with, ends with, is, is not,** and **is like**. The entry field will also be present in this example.

As another example, if you were to choose File in the first menu and one of the Date conditions in the second menu, the line changes to show two date-related menus, the first of which contains **before, after, exactly, not, on or before, on or after,** and **within**. The second date related menu contains **today, backup date,** and **specific date** (if you choose this, and entry field appears where you can enter the date).

As you can see, there are a large number of permutations available for each condition. Experiment with the menu choices to select the items that you want to include in the Rule.

First pop-up menu choice	Second pop-up menu choices
File Folder	Name Mac Path Windows Path UNIX path Attributes Kind Date accessed Date created Date modified Date backed up Size used Size on disk is (folder only) Size on disk is not (folder only) Label Permissions
Volume	Name Drive letter Connection type File system
Source Host	Name Login name
Saved rule	Includes Excludes

The “Saved rule” condition allows you to nest rules within rules. For example, to include the All Files Except Cache Files rule as a basis in your own custom rules, you would add the condition “Saved rule…includes…All Files Except Cache Files” in the Include criteria section beneath the “Any of the following are true” condition.

When you are done editing the Rule, click the Save button.

Exclude conditions always take precedence over Include conditions when Retrospect applies the Rule. For example, if a Rule has a statement which includes a user's Documents folder and a statement which excludes the enclosing Users folder, the files in the Documents folder will not be selected.

Duplicating Existing Rules

Sometimes it's easier to begin with and modify an existing Rule than to create a new one. To duplicate an existing Rule, select it in the list, then click the Duplicate Rule button below the list. Retrospect creates a new Rule named "old Rule name Copy." To modify the duplicate Rule, click the Edit Rule button. Make sure to change its name, then continue on to modify the Rule's criteria. When you are done making changes, click Save.

Deleting Rules

To delete a Rule, select the Rule in the list in Preferences, then click the Delete Rule button below the list, which looks like a minus sign (-). Retrospect asks you to confirm the deletion. Click the Remove button to eliminate the Rule.

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. Because everyone's situation if different, you will probably want to modify a strategy to better fit your needs. You may even devise your own strategy which is quite different from these suggestions. These strategies are just suggestions to help you get started, 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.

Basic Backup Rules

Retrospect is a powerful tool for safeguarding your data, but it's most effective when you follow some basic backup rules:

Back up often because you can't restore what isn't backed up. For example, if your hard disk malfunctions today but you most recently backed it up a week ago, you will 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 and schedules to automate backups.

Keep multiple backups of your data. Rotate among different Media Sets. Using more Media Sets makes you less likely to lose data if you misplace or damage media, especially if you are using tape or other removable media. Retrospect automatically keeps each Media Set complete and independent with its Smart Incremental backups, so there's no need to worry about outdated full, incremental, or differential backup methods.

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 button under Media Sets.

Retire old media on a regular schedule. Regularly introduce new mediaxe "media rotation;rotating media" using New Media 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 Media Sets based on what they contain and how often they get rotated and then label your media appropriately.

Always store at least one Media Set off-site to guard against fire, theft, and natural disaster. Update this Media Set at regular intervals.

Take care of your backup media, which can easily be damaged by the environment. Tape media can also wear out after as few as several hundred uses.

Back up the backup computer. You probably have put more time and energy than you realize into your Retrospect configuration.

Back up or copy your Catalog files to their own Media Set or another destination on your network. See "Catalog and Configuration Backups," later in this chapter.

Scripted Backups Versus Proactive Backups

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 running manual 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 or portable drives that appear on the network at random times.	Your network includes only desktop computers, no notebook computers or removable disks.
You want Retrospect to back up to whatever media is in the backup device.	The correct media is always available for unattended backups.

Your backup strategy will most likely be a combination of regular Backup scripts and Proactive Backup scripts. For example, you might choose to create Proactive Backup scripts only for the notebook computers, and use regular Backup scripts for the servers and desktop computers on your network.

Suggested Backup Strategies

There are a very large number of possible backup strategies, and they are limited only by your imagination and hardware. Here are some example strategies to get you started.

Regular Backups with Periodic Recycle

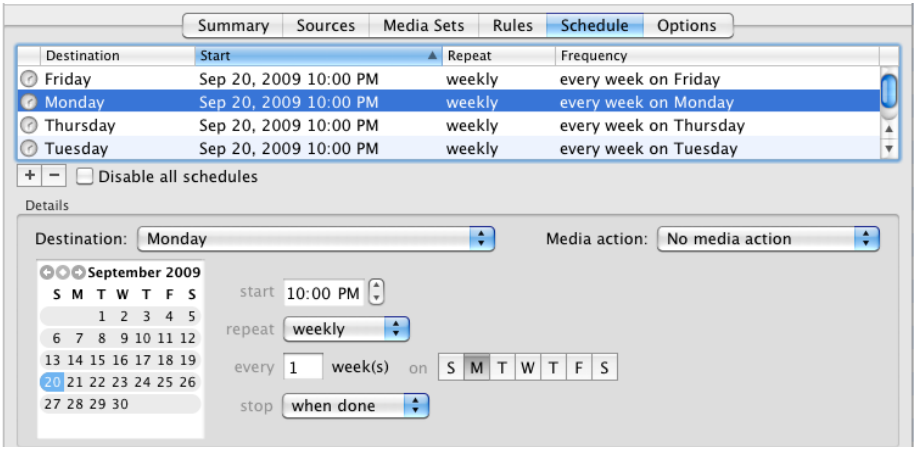
Create a Backup script to two rotating Media Sets. In the script's Schedule tab, add a schedule that repeats every other week at the same time, and select Monday through Thursday. Set this schedule to use the "No media action" media action to the first Media Set, so it does a regular backup. Add a second schedule that repeats once every other week (say on Friday) or monthly (say on the first of each month), and use the Recycle Media Set media action for the first Media Set. The second schedule will reset the Media Set and begin a fresh backup when it executes, keeping the overall size of the Media Set down. Then create two more schedules exactly like those above, only schedule them to run alternating weeks to the second Media Set. This strategy ensures that there is some amount of historical data (at least a week's worth) on one Media Set when the other is recycled and overwritten.

Five-day Backup Rotation

This strategy uses multiple Media Sets, one destination per workday. The idea is that you always have separate five-day rolling backups of your sources. The backup will run five days per week. Follow these steps:

1. Begin in the Media Sets category of the console by creating five destination Media Sets, named Monday, Tuesday, Wednesday, Thursday, and Friday. They can be any kind of Media Set, though the Disk kind will be most convenient.
2. In the Scripts category, create a new Backup script.
3. In the new script's Sources tab, choose the sources you wish to back up. You can choose from any of Retrospect's Source types: local volumes, Retrospect clients, network volumes, Tags, or Smart Tags.
4. In the script's Media Sets tab, click the checkboxes next to all five of the destination Media Sets that you created.

5. In the script's Rules tab, choose the Rule that you want to apply to the backups.
6. In the script's Schedule tab, create a schedule. Choose the Monday Media Set as the destination, and choose "No media action," which will back up all files and folders that have not been previously backed up to this Media Set. Choose a start time, and repeat the script every one week, selecting only the Monday button. Now Retrospect will do a backup every Monday to the Monday Media Set.
7. Repeat the previous step four more times, substituting a new day's Media Set as the destination and selecting the matching day in the Schedule tab. When you're done, you'll have five schedules for the script, each of which will execute once per week.



Tip: *It's good to have five different backups of your data, but it's even better if all of those backups are not to the same disk. Consider placing the members of each Media Set on two or even more disks.*

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 once per day.

Proactive Backup for Mobile Computers

Under the Tags tab of Sources, add a Tag called Mobile Computers. In the Sources list, select each of your Sources that are mobile devices, and apply the Mobile Computers tag. Remember that you can apply the tag to entire hard disks or to Favorite Folders, controlling the amount of data you will be backing up.

Next, create a Proactive Backup script. In the Sources tab of the script, select the Mobile Computers tag. When the script executes, Retrospect will back up all of the tagged Sources, saving you a lot of setup time because you don't have to select each mobile device separately. Schedule the new script to run twenty-four hours per day, with a backup interval of eighteen hours. (You never know when you're going to see a laptop again, and they're prone to breakage and theft, so it's rarely a bad idea to back them up more often.) Activate the "Allow early backup" option, so users who might be about to leave for a business trip can request an early backup.

Staged Backup Strategies

A *staged backup* is one in which you perform one or more backups to one kind of Media Set, and then copy those backups to a different Media Set, usually for archival purposes. The destination Media Set can be the same kind, or a different kind. For example, you could do a series of regular backups to a Disk Media Set, and then once per week (or once per month, or any other arbitrary time period you set) copy the contents of the Disk Media Set to a Tape Media Set. You can then file the tapes in your archival vault or other off-site facility.

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.

To create a staged backup with the above scenario, you need to create two scripts: your regular Backup script to a Disk Media Set, and a Copy Backup script to a Tape Media Set.

Begin by preparing the two Media Sets. Use a Disk Media Set with grooming enabled as the destination for the Backup script. Set the grooming option so that Retrospect keeps at least the last 10 backups for each source. This ensures that you will have a history of client data on disk for quick restores.

Create the Backup script. You may, of course, use an existing script. Set up a daily schedule for the backup.

Create a Copy Backup script to transfer the disk Media Set data to a tape Media Set once a week. In the Sources tab of the Copy Backup script, choose "Copy most recent backups for each source." In the Destinations tab, select the tape Media Set. Set the Rule that you want to apply to the script (for example, you might not care if your off-site archive set contains backed up operating systems and applications, so you would select the rule "User Files and Settings"), then add a weekly schedule. Every time the Copy Backup script runs, it will copy only new and changed files from the most recent backups contained in your Disk Media Set to the Tape Media Set. After the data in the disk Media Set has been copied to the Tape Media Set, you may take the tapes off-site for safe keeping, but don't forget to bring them onsite occasionally for an update!

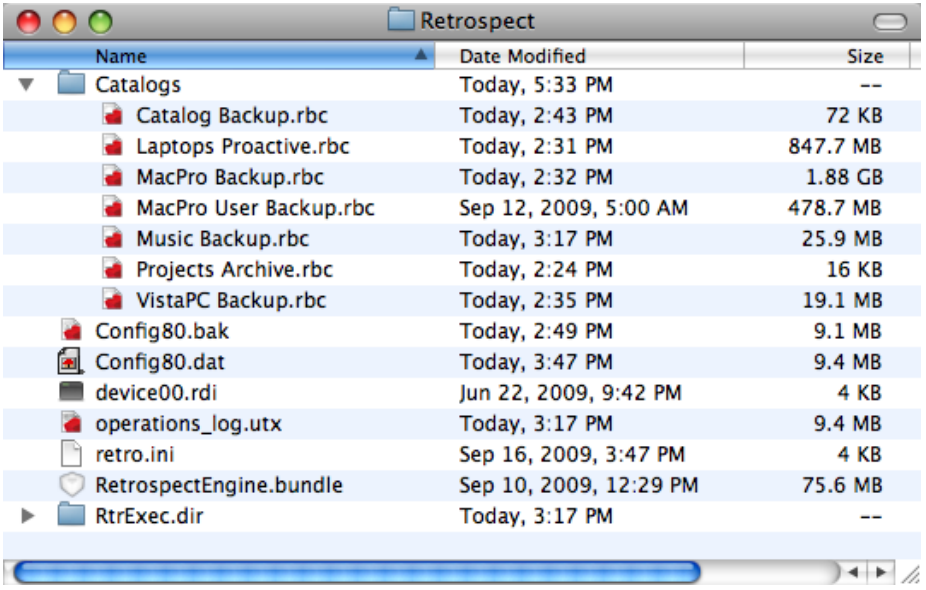
Catalog and Configuration Backups

Catalog files are the indexes to Media Sets, and they must be present for any operation involving a Media Set. By default, Catalog files are stored on the Retrospect backup server's hard disk. Since they reside on a hard disk, they face the same risks as your other files. If the Retrospect server's hard disk fails, and you lose your Catalog files, Retrospect cannot restore any files until the catalogs are recreated, which can be a lengthy process. It is always faster to restore an older version of a Catalog file and update it from the Media Set then it is to completely recreate a Catalog from the media. For this reason, you should back up your Catalog Files as well as your regular files.

The default location where Catalog Files are saved on the Retrospect server is `/Library/Application Support/Retrospect/Catalogs/`.

Similarly, Retrospect's configuration file contains your client database, scripts, schedules, preferences, custom rules, and other important information. Retrospect uses the configuration file, named `Config80.dat`, located at: `/Library/Application Support/Retrospect/`.

Periodically, Retrospect automatically saves a backup copy of `Config80.dat` in a file named `Config80.bak`. You should back up both of these files regularly. If your active configuration file becomes corrupt, stop the Retrospect engine, delete the `Config80.dat` file, then start the Retrospect engine, which creates a new configuration file from `Config80.bak`.



It's important to backup the Catalogs and configuration files regularly. Follow these steps:

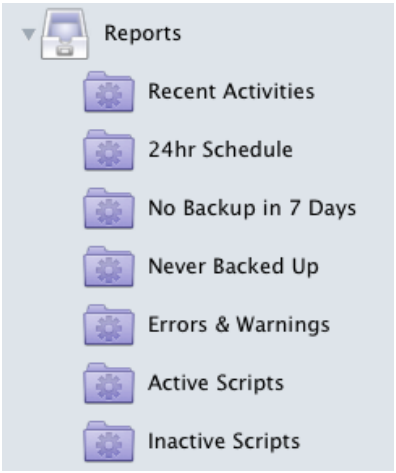
1. In the sidebar, click Sources.
2. In the Sources list, click to select the hard disk of the Retrospect backup server.
3. Click the Browse button. Retrospect will display a browse dialog showing the contents of the Retrospect backup server's hard disk.

4. Navigate to, then click to select `/Library/Application Support/Retrospect/`.
5. At the bottom of the browse dialog, click Add to Favorite Folders, then click Done.
6. In the sidebar, click Media Sets, then above the Media Sets list, click the Add button. Retrospect displays the Media Set dialog.
7. Choose the Media Set type, add a name for the Media Set, set any security you want for the Media Set, then click the Add button.
8. In the sidebar, click Scripts, then above the Scripts list, click the Add button. Retrospect displays the Script dialog.
9. Enter a script name (Catalog Backup is a good candidate), select All in the category list, then click Backup in the list of script types. Click the Add button. Retrospect returns you to the Scripts list.
10. In the detail area, click the Sources tab, then click the checkbox next to the Retrospect Favorite Folder you just created.
11. Click the Media Sets tab, then click the checkbox next to the name of the Media Set you created.
12. In almost all cases the default Rule of All Files will be what you want, so skip the Rules tab and click the Schedule tab. Add one or more Schedules to backup the Catalog and configuration files. As one possibility, you could create one schedule that executes every day at a particular time with no media action (which does a regular backup), and add a second schedule with a Recycle Media Set media action (which erases any previous backups and creates a new, fresh backup) once a month.

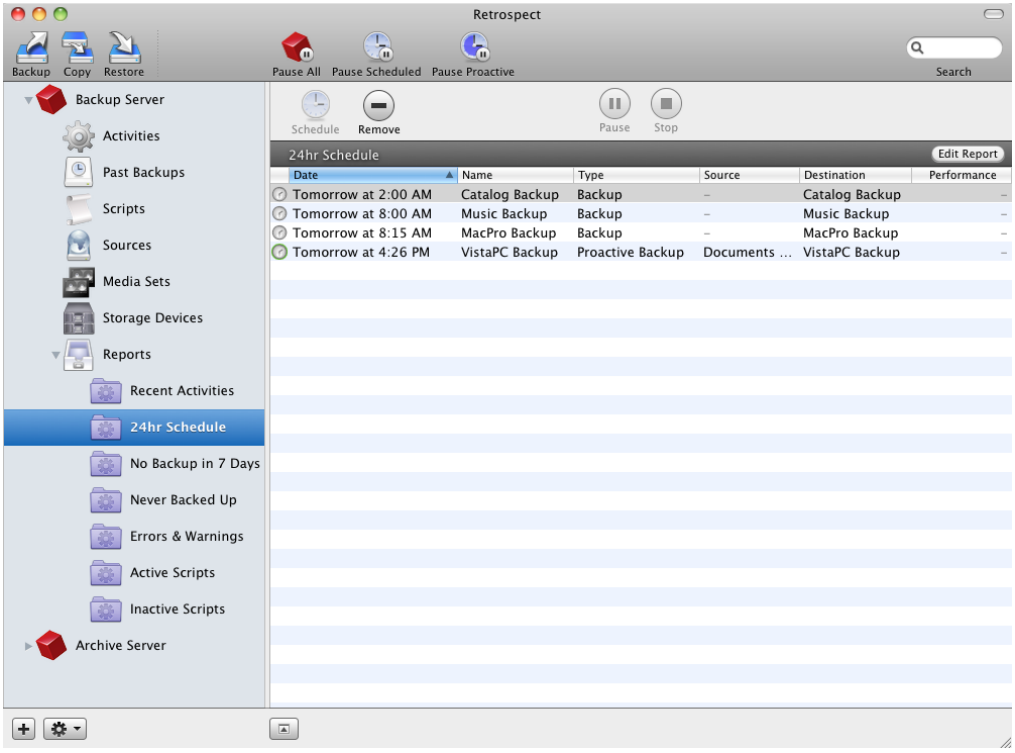
Working with Reports and the Operations Log

Retrospect's reporting abilities let you monitor backup 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.

Retrospect has a number of built-in reports, and you may also create your own. To see the reports, click the disclosure triangle next to Reports in the sidebar.



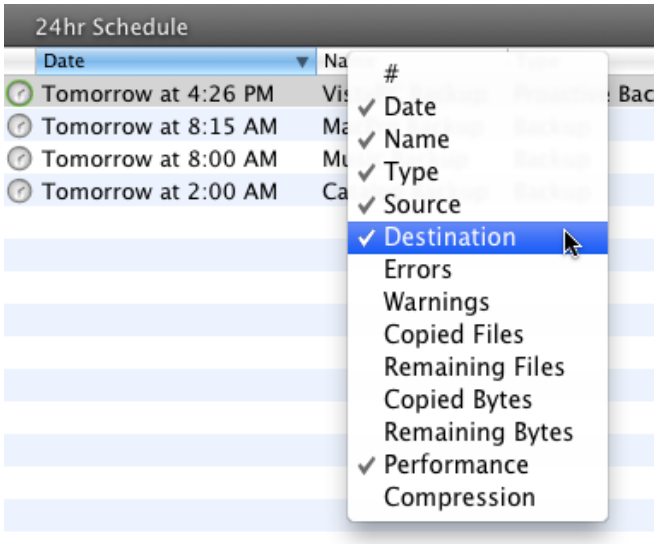
To view a report, click on one of the report names in the sidebar. The main part of the Retrospect window changes to display the report.



Customizing Report Views

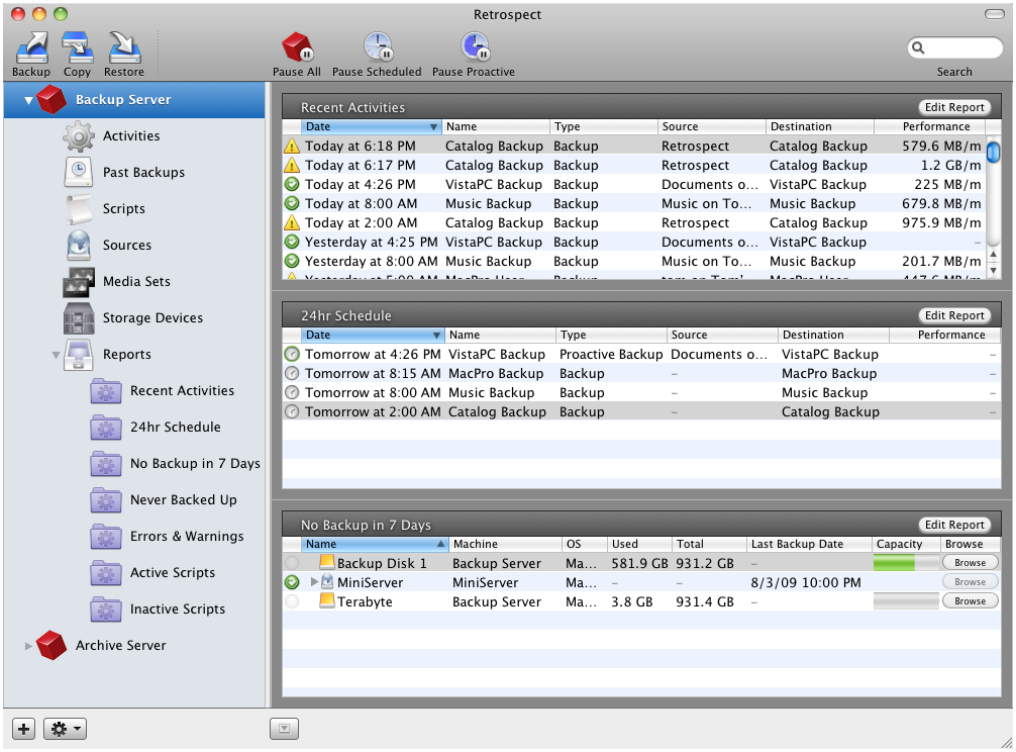
You can customize any report view. You may sort most columns in ascending or descending order by clicking the column header; a selected column is highlighted, and there is a upwards or downwards pointing sort arrow in the column heading. You may change the order of the columns in the list by dragging column headers. Clicking the line between the two columns allows you to drag to change the width of the column.

Different kinds of reports have different default columns. Besides these default columns, by right-clicking in any of the column headers, you get a contextual menu from which you may add additional choices to the list, or remove existing columns.



Using the Dashboard

When you launch the Retrospect console, it displays the dashboard, which is a overview of some of the reports that come with the program, as well as the ones that you have created yourself and chosen to display in the dashboard.



You can view the dashboard at any time by clicking on the name of the backup server in the sidebar. By default, the reports that appear in the dashboard are Recent Activities, 24hr Schedule, and No Backups in 7 Days. If you wish to add additional reports to the dashboard, select the name of the report in the sidebar, right-click, and choose Show in Dashboard from the resulting contextual menu.

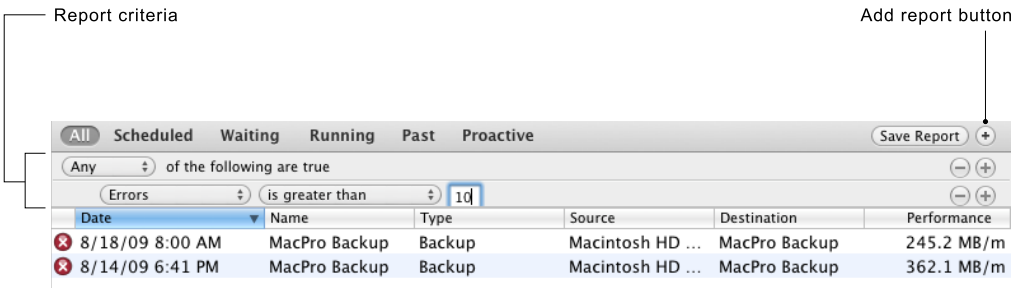
Note: *If you click on the Reports category in the sidebar, you get a dashboard-like view, but it includes all of the reports.*

Creating and Saving Reports

In Retrospect's sidebar, the Activities, Past Backups, Scripts, Sources, and Media Sets categories allow you to create custom reports. To begin, click to select one of the categories. As an example, we'll create a new report that alerts us when there are more than 10 errors in an operation.

Click on the Activities category, then click the plus (+) button in the scope bar to add the report and show the report criteria bar. Each category provides appropriate report criteria.

From the report criteria bar, choose the criteria you want, and if necessary, enter text or a number to narrow the scope of the criterion. You may add additional criteria by clicking the plus (+) button on the bottommost criterion. Holding down the Option key changes the plus (+) buttons to an ellipsis (...), which can be Option-clicked to add Any, All, and None conditions to the report criteria.



When you are done setting report criteria, click Save Report. In the dialog that appears, enter a name for the report, then click OK. The new report appears under the Reports category in the sidebar.

Editing Reports

To edit a report, click on the report's name in the sidebar, then at the top of the report, click the Edit Report button. The report criteria bar appears, with the existing criteria. Change any criteria you wish, then click Save Report. You can also edit a report by right-clicking on the report's name in the sidebar, and choosing Edit Report from the resulting contextual menu. The same menu also appears at the bottom of the sidebar as a tools menu with the gears icon.

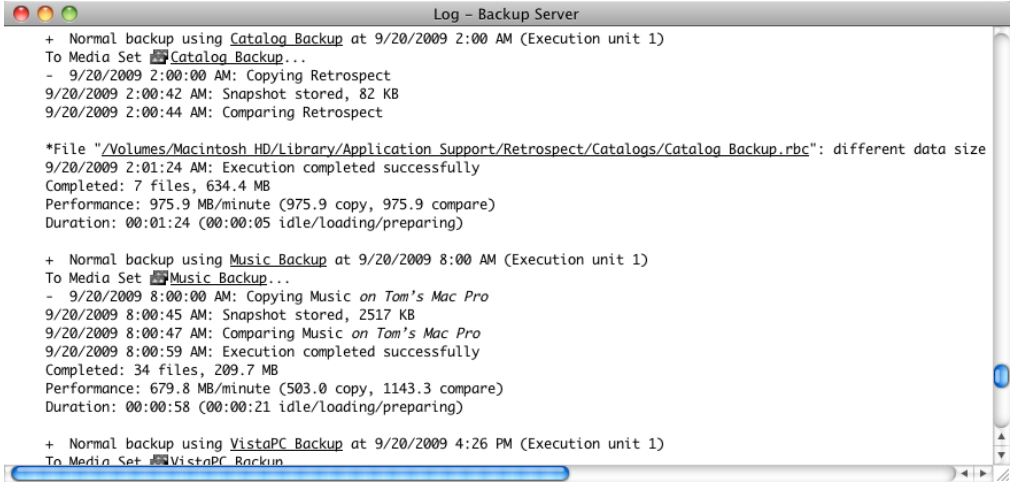
To duplicate a report, perhaps because you wish to use it as the base for a new report, right-click on the report's name in the sidebar, and choose Duplicate Report from the resulting contextual menu. Retrospect displays a dialog asking you to name the new report. Enter the name, then click OK. Then edit the duplicated report as needed.

To delete a report, select the report in the sidebar, then right-click and choose Remove from the contextual menu or choose Remove from the tools menu at the bottom of the Retrospect window.

Viewing the Log

The operations log shows a record of each Retrospect operation, transaction, and event, including any errors that occurred. The log stores messages that are generated during an operation. You may need to examine the log to find out why an operation was unsuccessful in order to diagnose problems.

To view the log, choose View > Log, or press Cmd-L.



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.

Performance indicates the number of megabytes of information copied per minute. If the Verification option 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.

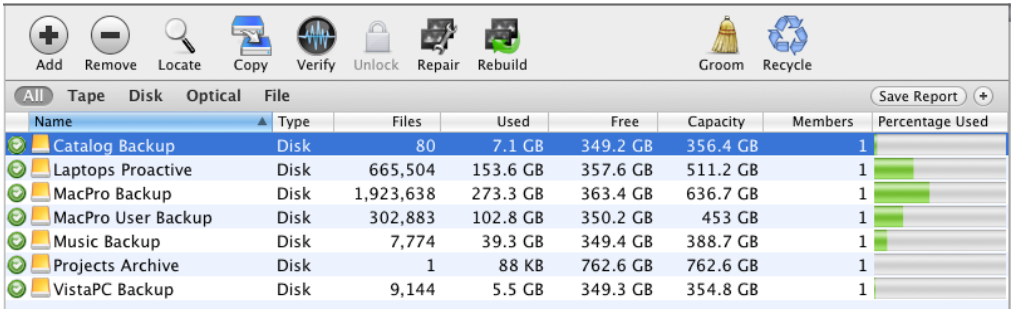
To find items in the log, when the log window is open, choose Edit > Find, or press Cmd-F. A search field appears at the top of the log window, with forward and back buttons next to it. Enter the text that you wish to search for in the search field. As you type, Retrospect shows you how many matches there are in the log for the search term.

Note: *You can choose how many lines you wish to appear in the operations log in the Console tab of Retrospect's Preferences.*

To print the Log, view it then choose Print from the File menu.

Managing Media Sets

Retrospect provides a number of tools to help you effectively manage your Media Sets. Choose Media Sets from the sidebar to view a list of the Media Sets and display the Media Set toolbar.



Name	Type	Files	Used	Free	Capacity	Members	Percentage Used
Catalog Backup	Disk	80	7.1 GB	349.2 GB	356.4 GB	1	
Laptops Proactive	Disk	665,504	153.6 GB	357.6 GB	511.2 GB	1	
MacPro Backup	Disk	1,923,638	273.3 GB	363.4 GB	636.7 GB	1	
MacPro User Backup	Disk	302,883	102.8 GB	350.2 GB	453 GB	1	
Music Backup	Disk	7,774	39.3 GB	349.4 GB	388.7 GB	1	
Projects Archive	Disk	1	88 KB	762.6 GB	762.6 GB	1	
VistaPC Backup	Disk	9,144	5.5 GB	349.3 GB	354.8 GB	1	

Creating New Media Sets

To create a new Media Set, click Create New. The process of creating a new Media Set is described in "Add Media Sets" in Chapter 5.

Removing Media Sets

You can remove a Media Set from the Media Set list by selecting it and clicking the Remove button. Click OK when prompted to remove the Media Set. Removing a Media Set does not affect the contents of the Media Set, nor does it delete its Catalog file. However, it does remove the Media Set from any scripts that use it.

As long as you don't delete the Catalog file and erase the media on which the Media Set is stored, you can always add the Media Set back to the list later. This process is described in "Rebuilding a Media Set," later in this chapter.

Adding a Media Set's Catalog

All Media Sets have a Catalog file, which serves as an index to the Media Set and allows Retrospect to find and restore data without needing to search through the entire Media Set. Retrospect keep its Catalog files on the Retrospect server machine, at `/Library/Application Support/Retrospect/Catalogs/`.

If you move a Media Set from one Retrospect server to another, you must add the Media Set's Catalog file so you can work with the Media Set. To do that, copy the Catalog file onto the Retrospect server, preferably into the default location (which will require admin-level authentication), so all of your Catalog files are in one place. Next, in the Retrospect console, click the Locate button in the Media Set toolbar. In the resulting dialog, navigate to the location of the Catalog you want to add, then click OK. Retrospect will ask you to enter the Media Set's password, if any. Enter it, then click OK to exit the password and navigation dialogs. Retrospect reads and stores the location of the Catalog file.

Note: *If you're moving a Retrospect server to a new machine, there are a few other things you must do. See "Moving Retrospect," later in this chapter.*

You can optionally perform a Verify operation with the Media Set to make sure that Retrospect knows how to access the actual media in the Media Set. See "Verifying a Media Set," later in this chapter.

Creating a Copy Media Set Script

Copy Media Set scripts allow you to make a copy of an entire Media Set onto different media. In the Media Set toolbar, there's an easy way to begin a Copy Media Set script. Select a Media Set from the list, then click the Copy button in the Media Set toolbar. Retrospect displays a dialog asking you to enter a name for the new Copy Media Set script, with a default name of "Copy Media Set -- *Media Set name*" already entered. Accept the default name or enter your preferred script name, then click Create.

Click on Scripts in the sidebar, and you will see in the Scripts list the new Copy Media Set script, with the Source of the script already selected. Finish setting up the script by adding the script's destination, rules, schedule, and options. For more information, see "Creating a Copy Media Set Script" in Chapter 5.

Verifying a Media Set

If you want to manually verify your Media Set, select the Media Set in the list and click the Verify button in the Media Set toolbar. Retrospect begins a Verify activity, which you can monitor by clicking the Activities category in the sidebar. During this activity, Retrospect scans the Media Set, verifying that it is readable and matches the Catalog file. The Verify feature is useful for performing offline verification of your Media Set media after an backup or archive that did not use verification.

Tip: *You should use Verify scripts to schedule offline verification if you want to maximize your backup window by running scripted backups (or archives) without verification.*

Whenever possible, a Verify activity verifies data on Media Set media by comparing the files in the selected Media 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 and speeds the overall operation.

In certain circumstances, Retrospect does not have access to MD5 digests generated during backup. This is true for all backups created when Retrospect's "Generate MD5 digests during backup operations" preference was disabled. In these cases, Retrospect still checks all files on the Media Set media to make sure that they are readable, though in this case their integrity cannot be guaranteed.

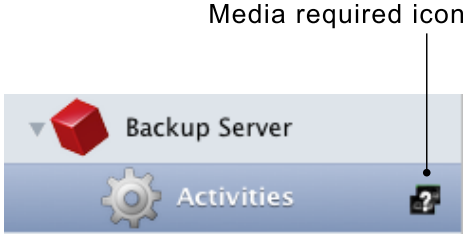
Note: *A* Verify *activity does require you to reinsert media when verifying backups that span media.*

To verify media integrity, follow these steps:

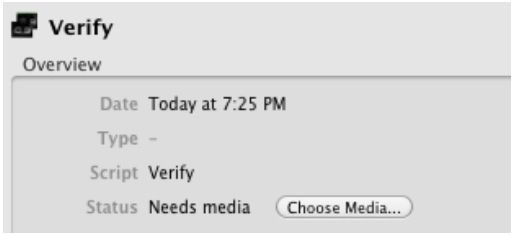
1. Select the Media Set you wish to verify, then click the Verify button in the Media Set toolbar.

   Retrospect verifies the Media Set media, informing you of its progress in the Activity list.

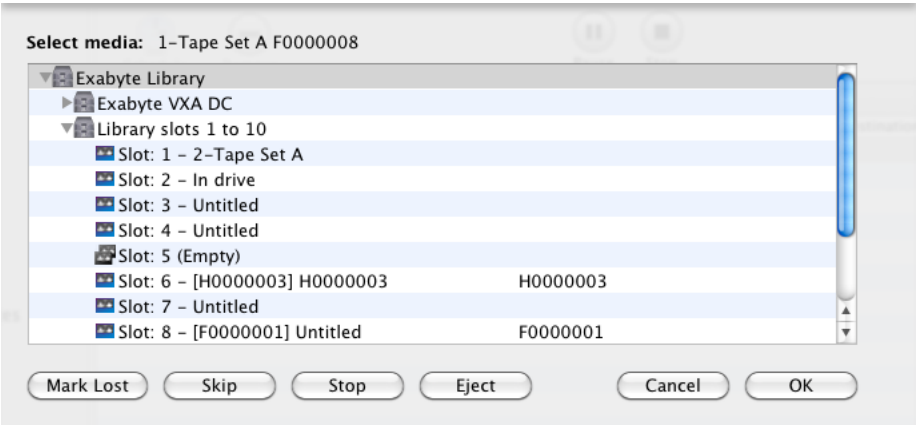
   If the Media Set uses tapes, optical disks, or removable disks, Retrospect asks you to insert each Media Set member as it is needed, alerting you to this by flashing the "media required" icon next to the Activities category in the sidebar. If you are verifying a Disk Media Set and Retrospect cannot find the members of the Media Set, you will also be asked to choose the location of the media.



Retrospect requests the media in the Detail section of the Activities list. Click the Choose Media button to bring up a dialog that allows you to navigate to the desired media.



This dialog appears differently, depending on the kind of Media Set you're verifying.



For tape and other kinds of removable media, if you do not have the requested Media Set member, but do have other members of the Media Set to verify, click Mark Lost, then insert the next requested piece of media. If the media is not lost, but is simply not immediately available, click Skip.

Note: *After a member of a Media Set is marked as lost, Retrospect will automatically try to reacquire all the files that were present on that member during any subsequent backups.*

2. When Retrospect finishes, click the Past button in the scope bar of the Activity list for details on whether the verification was successful. If

the operation was not successful or reported errors, click the Log tab for additional information.

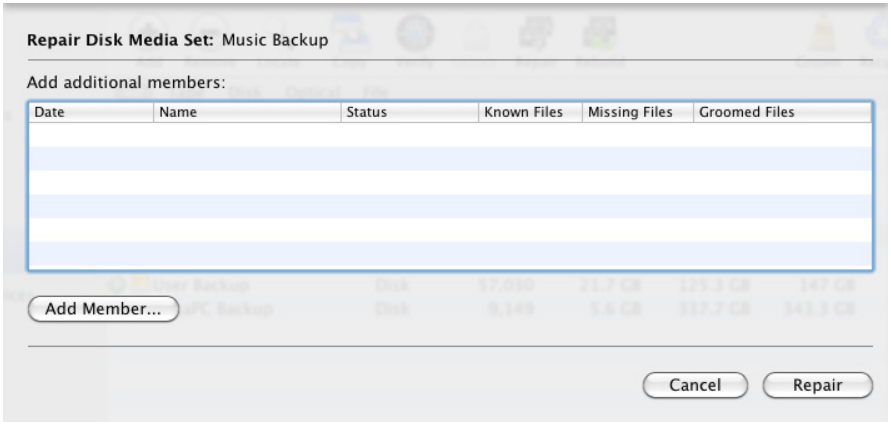
Repairing a Media Set

Occasionally, a Catalog file can become out of sync with the contents of its Media Set, such as when a power outage occurs in the middle of a backup operation. In this event, Retrospect will report a "Catalog out of sync" error. This is similar to losing your Catalog to a disk failure when you have a day-old copy of the Catalog file on another disk. In that case, you can copy the backup Catalog to the Retrospect server, then run the Repair feature to bring the backup Catalog back into sync with the media. Repairing the Catalog scans the Media Set and updates the Catalog file so that it matches the media.

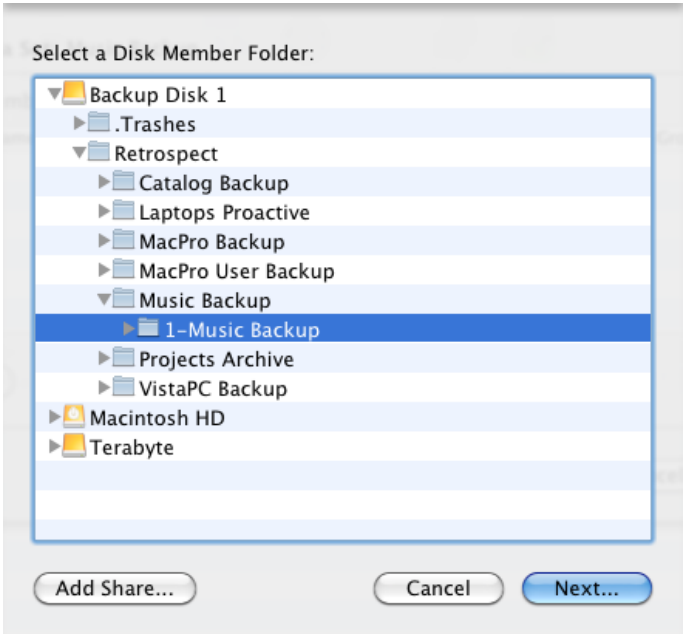
You must update the Catalog to synchronize it with the media or you will be unable to use the Media Set. A "Catalog out of sync" error indicates Retrospect was unable to update the Catalog the last time it copied data to this Media Set—-possibly because of a crash or power failure. This error may also be caused by a full disk or by a lack of memory.

To repair a Media Set, follow these steps:

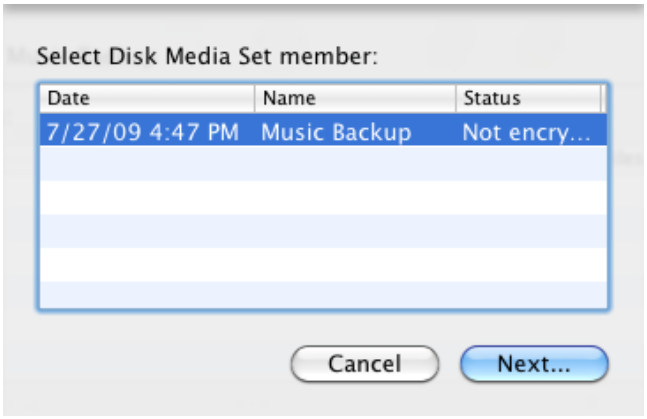
1. Select the Media Set you want to repair in the Media Set list.
2. Click the Repair button in the Media Set toolbar. Retrospect displays the Repair dialog, asking you to select the first member of the Media Set.



3. Click the Add Member button. Retrospect displays a dialog that allows you to navigate to the first member of the Media Set. In this example, using a Disk Media Set, we navigated into the Retrospect folder on our backup disk, then into the folder that contains the Media Set we wish to repair, and then we finally select the first member of the Media Set. It will always be named "1-Media Set name."



4. Click Next. Retrospect looks at the selected Media Set member, and displays a dialog showing the date, name, and status (encrypted or not encrypted) of the Media Set member.



5. Click to select the Media Set member in the dialog, then click Next. The Media Set member appears in the Repair dialog.
6. If there are additional members of the Media Set you need to add, repeat steps 3 through 5 until all members have been added.
7. Click Repair. Retrospect begins a Recatalog operation. You can monitor its progress in the Activities list. When Retrospect finishes, click the Past button in the scope bar of the Activity list for details on whether the recatalog was successful. If the operation was not successful, click the Log tab for additional information.

Rebuilding a Media Set

Rebuilding a Catalog recreates a fresh copy of the Catalog. A rebuild might be performed for a number of reasons, such as loss of the original due to disk failure. It scans the backup media and recreates the Catalog in its entirety.

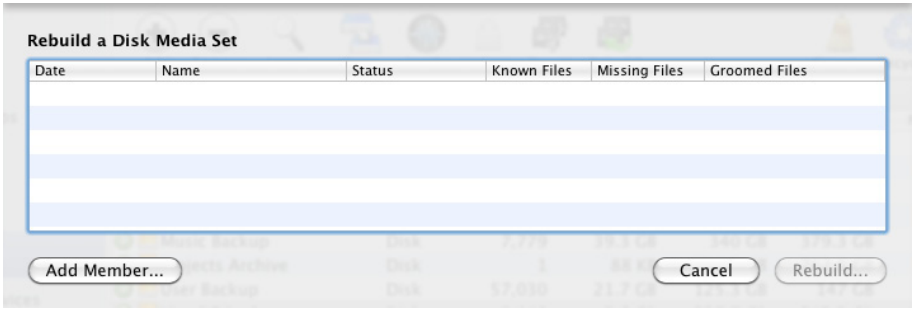
Note: *Retrospect has a feature, found in the Options tab of a Media Set, called Fast Catalog Rebuild where, every time it starts a tape after the first in a Media Set, it writes the current Catalog to the beginning of that tape. This speeds rebuilding of the Catalog by only requiring the last piece of media belonging to*

the Tape Media Set to be scanned by Retrospect. The Fast Catalog Rebuild option can also be used on Disk Media Sets that don't have grooming turned on.

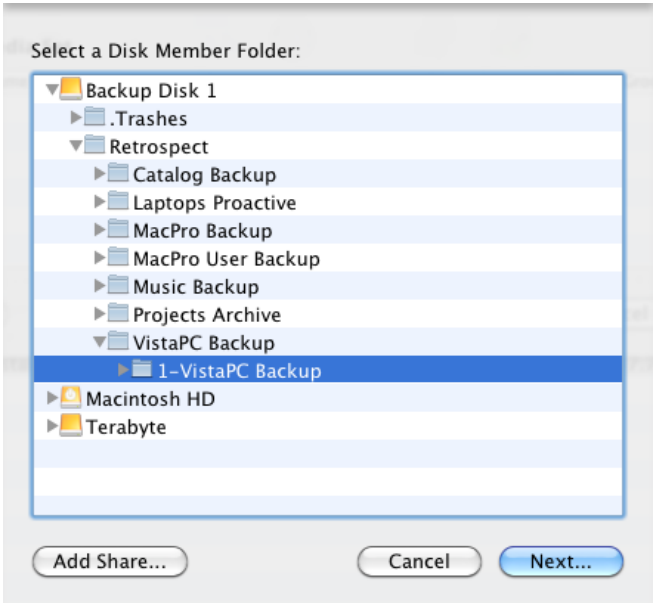
To rebuild a Media Set, follow these steps:

1. Select the Media Set you want to rebuild in the Media Set list.
2. Click the Rebuild button in the Media Set toolbar. Retrospect displays a dialog asking you what type of Media Set you would like to rebuild. Make your choice, then click Next.

3. Retrospect displays the Rebuild dialog, asking you to select the first member of the Media Set. The Rebuild dialog may be slightly different, depending on the type of Media Set you previously chose.



4. Click the Add Member button. Retrospect displays a dialog that allows you to navigate to the first member of the Media Set. In this example, using a Disk Media Set, we navigated into the Retrospect folder on our backup disk, then into the folder that contains the Media Set we wish to rebuild, and then we finally select the first member of the Media Set. It will always be named "1-Media Set name."



5. Click Next. Retrospect looks at the selected Media Set member, and displays a dialog showing the date, name, and status (encrypted or not encrypted) of the Media Set member.
6. Click to select the Media Set member in the dialog, then click Next. The Media Set member appears in the Rebuild dialog.
7. If there are additional members of the Media Set you need to add, repeat steps 4 through 6 until all members have been added.
8. Click Rebuild. Retrospect displays a dialog asking you to specify the folder where you want the rebuilt Catalog to be placed. Navigate to your desired location, select the folder, then click Rebuild. Retrospect begins a Recatalog operation, building a new Catalog file from the contents of the Media Set. You can monitor its progress in the Activities list. When Retrospect finishes, click the Past button in the scope bar of the Activity list for details on whether the rebuild was successful. If the operation was not successful, click the Log tab for additional information.

Grooming a Media Set

By default, when a disk that is a member of a disk Media 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.

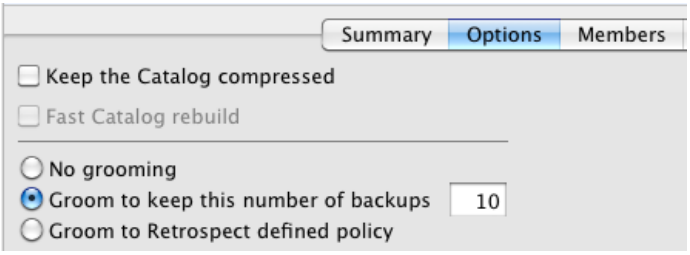
If you would rather continue to use the existing disk, you can use Retrospect's grooming options to reclaim disk space by deleting older files and folders to make room for new ones.

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.

Warning: As mentioned, grooming deletes files and folders to save disk space. These files and folders cannot be recovered. Before enabling grooming, make sure you have a backup policy that protects your critical files and folders.

Grooming Options for Disk Media Sets

These options are only available for Disk Media Sets. The selection you make tells Retrospect what to do when the Media Set to which you are backing up becomes full (or uses all the allotted disk space has been used). You can choose the disk grooming options in the Options tab of Media Sets.



The grooming options are:

- **No grooming:** 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.
- **Groom to keep this number of backups:** Specify the number of backups you want to preserve for each source when the backup drive fills up, or when you run a scripted or manual groom operation. Retrospect

then automatically "grooms" (i.e., deletes) all the other, older backups on the hard drive to make room for new data.

- **Groom to Retrospect defined policy:** When the backup drive fills up, or when you run a scripted or manual groom operation, Retrospect uses its own grooming policy to delete old backups. At a minimum, Retrospect's policy retains two backups for each source, saving the last backup of the day for each source from the two most recent days on which each source was backed up. Given enough space in the Media Set, 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.

Normally, you set a grooming option and need to do no more. But since you can turn grooming on or off for a given Disk Media Set at any time, you may have a nearly-full Media Set that you want to groom immediately after you enable grooming for the set.

Note: *When you activate grooming for a Media Set, Retrospect will retrieve the point-in-time file and folder listings from the Media Set for each source, going back as far as the number of backups you've set to keep in the grooming options, and add them to the Media Set's Catalog. Because Catalogs for Media Sets with active grooming policies need to store this additional data, they will be larger in size than Catalogs belonging to .*

To groom a Disk Media Set manually, select the Media Set in the list, and click Groom in the Media Set toolbar. Retrospect displays a dialog asking you to confirm the groom operation. Click Groom. Retrospect begins a Grooming operation, removing excess backups from the Media Set, according to the grooming options. You can monitor its progress in the Activities list. When Retrospect finishes, click the Past button in the scope bar of the Activity list for details on whether the grooming was successful. If the operation was not successful, click the Log tab for additional information.

Recycling a Media Set

When you perform a Recycle, Retrospect clears the Catalog file contents (if any) of the Media Set so it appears that no files are backed up. Then it looks

for the first media member of the Media Set and erases it if it is available. If the first member is not available, Retrospect uses any available new or erased media of the proper format. Everything selected from the source is backed up to the Media Set.

You can set a Media Set to be recycled with a script schedule, or manually in the Media Sets list. To Recycle a Media Set, follow these steps:

1. Select the Media Set you want to recycle in the Media Set list.
2. Click the Recycle button in the Media Set toolbar. Retrospect displays a dialog asking you to confirm the choice. Click Recycle.
3. Because the recycle will result in data loss, Retrospect asks you to confirm the operation again. Click Cancel or Recycle.

4. If you clicked Recycle, Retrospect deletes the contents of the Catalog file.

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, follow these steps:

1. Install the Retrospect engine and console on the new computer.
2. Gather the following files and folder from the `/Library/Application Support/Retrospect/` folder on the old Retrospect server and copy them to the Desktop on the new Retrospect server:

   `/Catalogs/` (the entire folder and its contents)

`Config80.bak`

`Config80.dat`

`operations_log.utx` (optional)

`privkey.dat` (if present)

`pubkey.dat` (if present)

3. On the new Retrospect server, use the Retrospect system preference pane to stop the Retrospect engine.
4. Copy the files and folder gathered in Step 2 to the `/Library/Application Support/Retrospect/` folder on the new Retrospect server, replacing the existing files. You may need to authenticate with an administrator password to complete this operation.
5. Correct the ownership of the files you just moved by opening the Terminal application and carefully entering the following commands and authenticating with an administrator password:

   ```
   cd /Library/Application\ Support/Retrospect/
   sudo chown -R root:admin *
   ```

   Warning: *Be certain that you have changed to the proper directory with the cd command before executing the chown command. After entering the cd command, the Terminal prompt should be* `machineName:Retrospect username$`. *If it's something different, try entering the cd command again.*

6. Use the Retrospect system preference pane to start the Retrospect engine on the new Retrospect server.
7. Next, you must force the new Retrospect server to recognize the Catalog files you just moved. In the Retrospect console's Media Sets category, highlight all the Media Sets with red X icons in the Status column and click the Remove button. Then click the Locate button and follow the steps described in "Adding a Media Set's Catalog," earlier in this chapter for each Catalog file that you copied to the new Retrospect server.
8. 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. Remove 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. In Sources, remove the previously local volumes. Removing volumes removes them from the volumes database and any scripts which use them.

Chapter 8: Troubleshooting and Support Resources

This chapter offers solutions to problems you may encounter with Retrospect, as well as basic troubleshooting suggestions. You'll also find procedures for getting help from our Technical Support staff.

Troubleshooting Retrospect

Most problems encountered while using Retrospect fall into a few general categories. 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 suggests you the first steps you should try, then shows you where to get more help.

Tip: *The very first thing you should do when you encounter an error is to make sure that your version of Retrospect is up-to-date. From the Retrospect menu, choose Check for Retrospect Updates. Install the latest updates to see if they resolve your problem. Don't forget that you may need to install updates for both the Retrospect console and the Retrospect engine.*

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, later in this chapter.

Troubleshooting Process

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 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 at a particular phase of the backup or restore process, you are on your way toward solving it.

Things to Try First

There are a few simple actions you can try that often solve problems.

On the Retrospect Server

Stop and start the Retrospect engine.

Follow these steps:

1. Make sure all instances of the Retrospect console are closed, whether those are on the Retrospect server machine or on a remote machine.
2. From the Apple menu, choose System Preferences > Retrospect.
3. In the System Preferences window, click Retrospect.

4. In the Retrospect preference pane, click the lock in the lower-left corner, then enter your administrator password and click OK.
5. Click Stop Retrospect Engine. Wait until the message in the window states the "Retrospect Backup Engine is currently stopped." It could take several minutes to stop the engine in some cases. Click the button again, which now reads Start Retrospect Engine. You will need to authenticate with your password again.
6. Check to see if the problem has been resolved.

Tip: *On rare occasions, the Retrospect engine will not be able to be stopped using the preference pane. In this event, use Activity Monitor (found in* `/Applications/Utilities/`*) to Force Quit the RetroEngine process.*

Restart backup hardware devices.

Backup devices such as tape drives and tape libraries can sometimes lose contact with the Retrospect server. If the backup device does not appear in the Retrospect console, stop the Retrospect engine. Then try turning the device off and on again. Then start the Retrospect engine again.

Note: *SCSI devices should only be turned off when the computer is turned off. Hard disks should be ejected from the desktop before turning them off and on again.*

On a machine running the Retrospect console

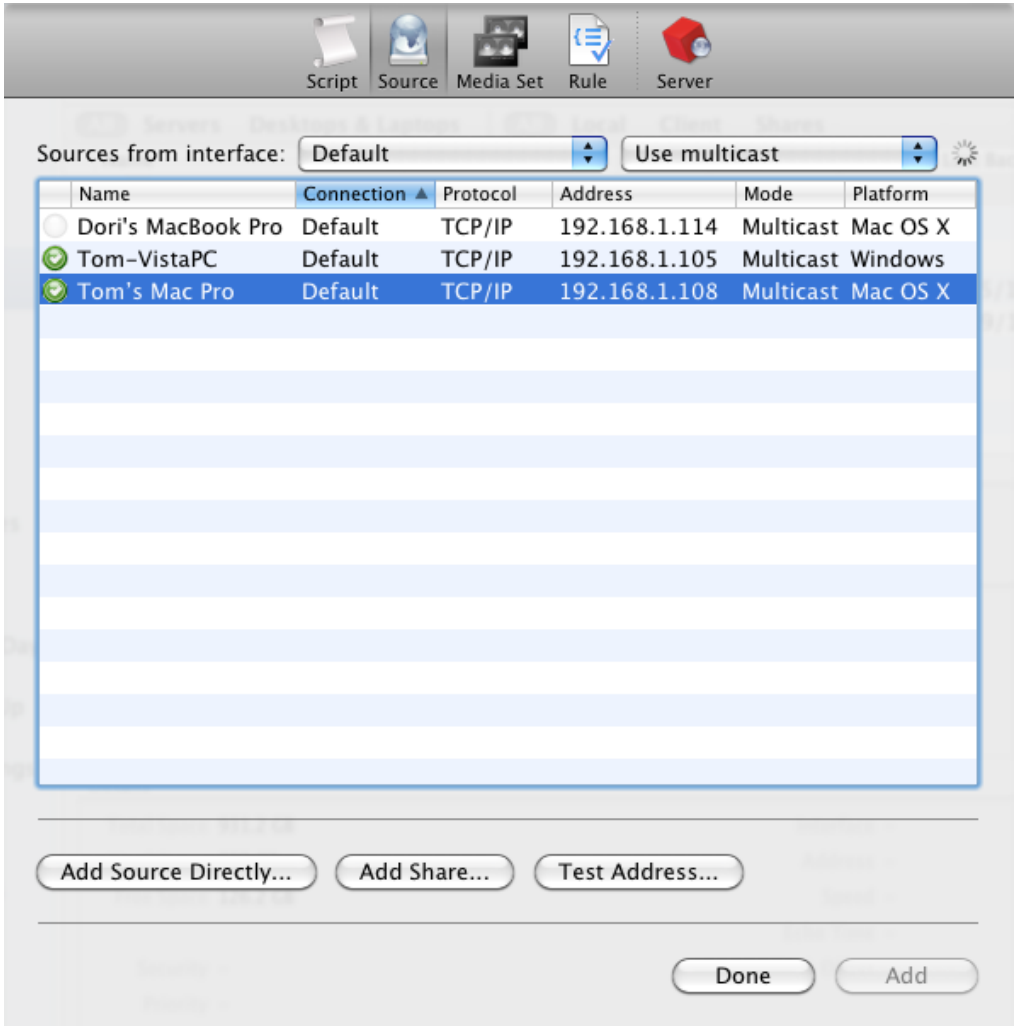
If the console does not see the Retrospect server:

1. Make sure that the Retrospect engine is actually running on the Retrospect server.
2. Make sure that the Retrospect server machine's networking is correctly configured.
3. Quit and restart the Retrospect console application.

If a client in the local subnet or in another Retrospect-configured subnet doesn't appear in Retrospect's Sources view, or appears intermittently:

Use the Test Address button in the Add Sources dialog to see if the client is on the network. Follow these steps:

1. Click Sources in the console's sidebar, then click the Add button in the Sources view's toolbar. The Add Sources dialog appears.
2. Click the Test Address button. In the resulting dialog, enter the address of the source you want to test. You can enter the IP address, the DNS address, or the local hostname. Click Test. If the client responds, Retrospect will show you the client's name, address, and client software version. If the client is not reachable, Retrospect will display an error message.


Script
Source
Media Set
Rule
Server
Sources from interface:
Default
Use multicast
Name
Connection
Protocol
Address
Mode
Platform
Dori's MacBook Pro
Default
TCP/IP
192.168.1.114
Multicast
Mac OS X
Tom-VistaPC
Default
TCP/IP
192.168.1.105
Multicast
Windows
Tom's Mac Pro
Default
TCP/IP
192.168.1.108
Multicast
Mac OS X
Add Source Directly...
Add Share...
Test Address...
Done
Add

On the Retrospect client machines

If a client machine does not appear in the Retrospect console:

1. 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."
2. Make sure the client computer is connected to the network and its network settings are correct.

Getting more help

If none of these basic measures solve your problems, first refer to the Retrospect Knowledgebase (Help > Online Knowledgebase). If you still cannot diagnose and solve the problem, please contact Retrospect Technical Support.

Retrospect Support

Retrospect provides built-in access to a number of useful resources. From the Retrospect Help menu, you can access:

- **View Retrospect Quick Start Guide.** Get up and running quickly using Retrospect.
- **View Retrospect 8 Read Me.** Tips, late-breaking information, known issues, and workarounds.
- **Retrospect website.** Retrospect's home on the Internet. To access Retrospect's website directly, go to `http://www.retrospect.com`.
- **Retrospect Support.** Support section of the Retrospect website. Includes links to tutorials, user forums, etc. To access the support section directly, go to `http://www.retrospect.com/supportupdates/`.
- **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 `http://www.retrospect.com/knowledgebase/`.

- **Online Video Tutorials.** Short videos detailing how to accomplish common tasks with Retrospect.
- **Supported Devices.** Searchable backup hardware compatibility database provides information of which devices Retrospect supports. To access supported devices information directly, go to `http://www.retrospect.com/supporteddevices/`.

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, Retrospect Technical Support is available to help. To learn more about available support options, check Retrospect's support matrix at `http://www.retrospect.com/supportupdates/service/support/`.

For information about contacting Technical Support in the U.S. and Canada, as well as internationally, see `http://www.retrospect.com/supportupdates/service/`.

Before you Call Technical Support

In the event you need to contact our Technical Support staff, we can serve you best if you gather some information first. We suggest that you follow these steps:

Have the following information ready:

- The version of Mac OS X for the Retrospect server, the machine on which you are running the Retrospect console, and any involved Retrospect client machines
- The exact version of Retrospect
- The amount of RAM on the Retrospect server machine
- The types of backup devices you are using that are connected to the Retrospect server

You should be at the Retrospect server and running the Retrospect console when you call.

You should also be prepared to answer the following questions:

- Check the Retrospect Operations Log (View > Log). Are you getting a specific error message? Please note and report to the technician any error messages that appear in the log.
- When does the error happen? During backup, restore, copy, compare, or working with the Retrospect console?
- Is this a local backup, or is it a backup of a client computer?
- What troubleshooting have you tried so far?
- Has this worked for you in the past, or is this an ongoing problem?
- How often does the problem occur?
- Are there any crash logs or errors in the Mac OS X Console?

The answers to these questions may help you troubleshoot further by suggesting avenues you haven't already tried. They will certainly help the Retrospect Technical Support Staff help you find a solution.

Glossary of Terms

access privileges – The privileges given to (or withheld from) users to see folders, see files, and make changes to shared volumes.

activity thread – A term used to indicate the separation of multiple, concurrent activities. When Retrospect runs an activity, such as a backup or a restore, it runs that activity in a thread separate from other activities. Generally, each activity requires a unique source and destination. By assigning activities to the same activity thread, it ensures that they will run one after the other.

append – To write additional data to a Media Set. With a Smart Incremental Backup, Retrospect appends file data to the current Media Set member.

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 Media Set is an archive. Also see Media Set.

archive (verb) – To copy files from a volume to a Media Set. For example, "Let's archive these QuickTime movies." Archiving may, optionally, involve removing the copied files from the source. Also see back up.

back up (verb) – To copy files from a volume to a Media 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. A complete, point-in-time state of a volume backed up by Retrospect that includes a file and folder listing of all files present at the time of the backup, any metadata related to those files, and any actual files necessary to restore that volume. Retrospect's backups of Windows computers may also contain System State information. Retrospect stores its backups in Media Sets. 2. An operation in which files are backed up. For example, "I just ran today's backup." 3. An entity of backup materials. For example, "Fortunately, we can get the backup from the safe and restore the files." Also see *back up*, *Media Set*, and *metadata*.

backup date – The most recent date and time a Mac OS file, folder, or volume was copied to a Media Set. Retrospect does not rely on this date and will only set this

date for volumes, folders, and/or files when you check the appropriate boxes in the Macintosh client options. Also see creation date and modification date.

Backup Set – Previous editions of Retrospect use this term to describe one or more pieces of media that contain the backups. See *Media Set*.

browser – Retrospect's tool that allows you to view the folder and file structure of a volume or contents of a Media Set. You can also use a browser to see the files and folders in a Media 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 Media Set. The Catalog file allows you to mark files for restore or retrieval without having to load or insert your Media Set media.

client – A networked Windows, Linux, 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 Media 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 rules, a distinguishing criterion relating to file or folder characteristics, such as name or creation date. You can choose multiple conditions to make your own custom rules. Also see *rules*.

Config80.dat file – The file containing your custom settings, including known Media 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.

console – The Retrospect application, which provides control and monitoring capabilities for one or more Retrospect servers running the Retrospect engine. The Retrospect console can control and monitor Retrospect servers over a TCP/IP network, so it need not be installed on the same computer as the Retrospect engine. Also see *engine* and *Retrospect server*.

copy (noun) – 1. A replica of one or more files and folders that perfectly match the original files and folders. 2. An operation in which files are copied from one location to another, as in a Copy script. Retrospect's copy operation can make an exact copy of a volume, including that volume's ability to start up (boot) a computer. Previous versions of Retrospect called copy operations "duplicate" or "transfer" operations.

copy (verb) – To create an exact duplicate of an original. Retrospect can copy volumes, such as when making a bootable copy of a Mac OS X startup disk, and it can also copy backups from one or more Media Sets to another.

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. Mac OS X 10.6 "Snow Leopard" discontinued the use of creator codes. Retrospect lets you select files according to creator code, if present.

deduplication – A method for reducing the amount of data stored in a system by eliminating redundant data, replacing it instead with a pointer to the first-stored copy of that data. Retrospect employs a method of deduplication known as file-level deduplication or single-instance storage. Retrospect

destination – The storage medium to which files are being moved, copied, or otherwise transferred. When backing up or archiving, the destination is a Media Set. When restoring or copying, the destination is a volume.

device – Any piece of peripheral equipment connected to your computer, such as a hard disk drive, removable cartridge drive, or tape drive. In this manual, the term "backup device" refers to any device that accepts Media Set media, such as a removable cartridge 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 booting from an alternate startup disk (or installing a temporary OS) and then restoring the entire hard disk from a Retrospect backup.

disk – Retrospect uses the term disk to refer to fixed disks, network volumes, or removable disks (e.g., RDX, Rev, MO). This manual uses the term disk in two contexts: 1. as an accessible volume for general storage; and 2. as a medium for use in a Disk Media Set.

disk-to-disk-to-disk (D2D2D) – A staged backup methodology that stores regular backups of data from hard disk drives on a primary disk-based backup storage system, followed by copying some or all of the backed up data to a secondary disk-based backup storage system at some specified interval. For example, nightly backups may be stored on a network-attached storage device that gets offloaded to a secondary disk system located offsite once a week.

disk-to-disk-to-tape (D2D2T) – A staged backup methodology similar to D2D2D that stores regular backups of data from hard disk drives on a primary disk-based backup storage system, followed by copying some or all of the backed up data to a tape storage system at some specified interval.

Disk Media 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.

engine – The background process (RetroEngine) responsible for running Retrospect's backup and recovery operations, communicating with client computers, and controlling storage devices. A computer running the Retrospect engine is called a Retrospect server and must be controlled via the Retrospect console. Also see *console* and *Retrospect server*.

File Media Set – This type of Media Set combines the Catalog and the data in a single file. The Media Set media must be a single volume that is accessible from the Mac OS X Finder, such as a file server or hard disk. Also see Backup Set.

grooming – An option for Disk Media Sets. Retrospect automatically deletes older files and folders from the Disk Media Set when it runs out of disk space, or on a user-set schedule, in order to make space available for newer backups.

Favorite Folder – A folder you designate as an independent volume for use within Retrospect. Previous versions of Retrospect used the term Subvolume.

live restore – A restore operation that overwrites the files belonging to an operating system while the computer is started up from that operating system. A live restore is often used to roll a system back to a previously backed-up point in time, or in the case of disaster recovery after a temporary operating system has been installed on the computer being restored.

local subnet – The subnet in which the backup computer resides.

matching – The scheme for comparing file attributes to determine whether files are identical, which then allows intelligent copying to avoid redundancy. Also see Smart Incremental Backup.

media action – A setting that determines how Retrospect will use media during a backup. "No media action" tells Retrospect to append data to last member of the Media Set; if the Media Set is empty, Retrospect uses the first member. "Skip to new member" tells Retrospect to use the next available empty media. "Start new Media Set" allows you to periodically introduce new media into your backups, keeping the original Media Set media and Catalog intact for archival purposes. It tells Retrospect to create a new Media Set with an incremented name (for example, Disk Set A would become Disk Set A [001]), to change all scripts that pointed at the original to point to the new set, and finally to run the activity to the new Media Set. "Recycle Media Set" tells Retrospect to delete the contents of the selected Media Set's Catalog, then erase and reuse the first member of that Media Set, literally recycling the media and using it over again. Note: A recycle media action is destructive, the other media actions are not.

Media Set – Retrospect stores all files in Media Sets. There are different types of Media Sets for different media and devices: Disk Media Sets for removable and fixed disks, File Media Sets for a single volume, and Tape Media Sets for tape cartridges.

medium – Any hard drive, disc, tape, or cartridge to which files can be copied. In this manual, media usually refers to the media belonging to a Media Set.

member – An individual medium (such as a disk, tape, or cartridge) used in a Media Set.
metadata – Information about the files and folders stored in a file system, such their names, when the files were created, what their size is, and which users can access them. Retrospect uses metadata to determine the uniqueness of files

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.

Open File Backup – Retrospect's Open File Backup for Windows Clients add-on allows files to be backed up even if they are opened and being used. This is important to ensure proper backup of Windows server applications such as customer relationship management applications and accounting packages, which often run 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 launches, executions, errors, and completions, as well as information on the number of files copied, duration of backup, and backup performance.

path – The fully specified name of a computer file, including the position of the file in the file system's directory. For example, in Mac OS X, the path of the Network Utility application is: `/Applications/Utilities/Network Utility.app`. Also referred to as pathname.

Piton – Retrospect's own proprietary PIpelined TransactiON 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.

selecting – Selecting files in the browser to be backed up or restored. Files can be selected (or deselected) manually, or they can be selected according to various criteria using rules. In the browser, a check mark appears next to any selected file. Files that are only highlighted in a browser are not necessarily selected. Pervious versions of Retrospect referred to selecting as marking.

server – A computer running server software, such as Mac OS X Server or Windows Server 2008.

Smart Incremental Backup – A backup that intelligently copies only files that aren't already stored in the destination Media Set. Every Smart Incremental Backup is like a virtual full backup, such that it allows for precise point-in-time restoration of any backed-up volume. Retrospect always performs Smart Incremental Backups. Also see *deduplication* and *matching*.

report – Specially configured layouts of Retrospect's list views that present useful information on a variety of components in the overall backup environment. You can use Retrospect's built-in reports and create your own.

restore – An operation which copies files from a Media Set to a volume.

Retrospect server – a computer running the Retrospect engine where backup devices are typically connected. Also see *console* and *engine*.

root – 1. The highest level of folders in a data structure. When you select a drive icon in the Mac OS X Finder or Windows Explorer, you see the root folders and files. Also denoted on Mac and Linux systems by the first slash (/) in a path. 2. The superuser account on Mac OS X and Linux systems. The Retrospect engine and Retrospect Client software run as root processes, with full access to the file systems with which they interact.

schedule – A script element that lets you schedule a script to automatically execute at dates and times of your choice.

script – A saved 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 in Retrospect.

rule – A feature that lets you search for or filter files which match certain conditions, such as All Files Except Cache Files. You can use Retrospect's built-in rules and create your own.

scope bar – A Mac OS X user interface element that allows for the placement of scope buttons. Also see *scope button*.

scope button – A button that allows you to manipulate or narrow the focus of a search or display listing. As an example, the "Scheduled" scope button in Retrospect's Activities view changes the scope of the items displayed in the list view such that only scheduled (upcoming) activities will be shown.

session – In previous versions of Retrospect, a group of files from a single operation stored within a Media Set. Retrospect 8 now uses the term *backup* to include both session and Snapshot data. Also see *backup*.

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 – In pervious versions of Retrospect, a Snapshot refers to the point-in-time file and folder listing that is captured during a backup operation to depict a volume's state (that is, all its files and their paths). Makes it easy to restore a hard disk to its exact state as of a given backup. Retrospect 8 now uses the term *backup* to include both session and Snapshot data. Also see *backup*.

source – In a backup, duplicate, or archive operation, the volume from which files are copied. In a restore, the Media 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. Also see *disk-to-disk-to-disk* and *disk-to-disk-to-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 – In previous versions of Retrospect, a folder you designate as an independent volume for use within Retrospect. Retrospect 8 uses the term *Favorite Folder*.

Tape Media Set – For use with tape drives. Also see *Media Set*.

TCP/IP – Transmission Control Protocol/Internet Protocol. An industry-standard network protocol and the standard protocol of the Internet, web servers, and FTP servers. It is the protocol used by Retrospect to communicate with Retrospect clients.

volume – A hard disk, partition of a hard disk, Favorite Folder, file server, or any data storage medium that is logically recognized by Retrospect as a file and folder storage location.

Index

D

E

F

G

H

I

L

S

T

U

V

W