

Retrospect Backup 19

Mac User's Guide



Protecting data since 1989. © 2024 Retrospect. All rights reserved.

Retrospect Backup 19 Users Guide, first edition.

Use of this product (the “Software”) is subject to acceptance of the license agreement presented in the installer. You may not install, copy or otherwise use the Software except as expressly provided in that license agreement. Retrospect is a registered trademark of Retrospect in the United States and/or other jurisdictions. All other trademarks are the properties of their respective owners.

Contents

- What's New 5
 - Retrospect Cloud Storage 5
 - Backup Comparison 7
 - Cloud Performance Improvements 8
 - LTO-9 Tape Support 8
 - Multi-Factor Authentication (MFA) and Encryption 9
 - Support for Microsoft Azure for Government 10
 - Flexible Immutable Retention Periods 11
 - Bug Fixes 14
- Quick Start Guide 15
 - First Launch Experience 15
 - Backup 16
 - Restore 21
- Introducing Retrospect 25
 - Overview of Retrospect 25
 - Installing Retrospect Backup 28
 - Upgrading from Previous Versions of Retrospect 30
 - Upgrading from Retrospect 6.1 30
 - Stopping and Starting the Retrospect Engine 31
 - Starting and Stopping the Retrospect Console 31
 - Overview of the Retrospect Console 32
 - Retrospect Dashboard 35
 - Enabling "Full Disk Access" 37
 - Security and Encryption 39
- Fundamentals 41
 - How Retrospect Works 41
 - Sources 41
 - Media Sets 42
 - Storage Groups 44
 - Media Actions 48
 - Catalog Files 48
 - Retrospect Clients 49
 - ProactiveAI Backup 49
- Hardware 52
 - Sources and Storage Devices 52
- Working with Clients, Servers, and Network Shares 70
 - Network Backup Overview 70
 - Client Licenses 70
 - Working with Retrospect Clients 71
 - Client Security 72
 - Network Interfaces 73
 - Adding Retrospect Clients to Sources 73
 - Testing Client Connectivity 74

Removing a Client	75
Getting Information About a Client	75
Updating Clients	77
Uninstalling a Client and Its Software	78
Working with Servers and Network Attached Storage	78
New Retrospect Client software	79
User-initiated backups and restores	80
Locking client features and preferences	83
Advanced Networking	84
Network Backup Guidelines	88
Working with Retrospect	91
Preparing for Retrospect Operations	91
Backing up	92
Working with Activities	100
Pausing Global Retrospect Operations	102
ProactiveAI Backup	49
Copying (Replication)	106
Archiving	108
Restoring	110
Working with Schedules	113
Working with Utility Scripts	114
Filtering the contents of a past backup	120
Cloud Backup	121
Amazon S3 Account Setup Guide	121
Storage Setup Guide	125
Choosing a Storage Class	129
Simple Access Setup Guide	135
Advanced Access Setup Guide	135
Information for Retrospect	140
Adding Cloud Storage in Retrospect	140
Using Cloud Storage in Retrospect	142
Throttling Cloud Backups in Retrospect	143
General Tips	145
Ransomware Protection	146
Overview	146
Step-by-Step Guide	146
Technical Details	149
Anomaly Detection	151
Overview	146
Detecting Anomalies	151
Step-by-Step Setup Guide	153
Retrospect Cloud Storage	157
Overview	146
Tiers	157
Setup	157

Security Reporting.....	160
Reporting Functionality	160
Geo Tracking Endpoints	162
Cloud Data Protection.....	164
Information for Retrospect	140
Step-by-Step Guide	146
Account Setup Guide	169
Storage Setup Guide	125
Cloud Deployment	177
Account Setup	177
Instance Setup	181
Remote Backup	182
Virtual Private Cloud (VPC)	184
Disaster Recovery	185
Overview of Disaster Recovery	185
Preparing for Disaster Recovery	185
Workflow for macOS El Capitan and Higher	186
Workflow for macOS Mavericks and Lower	188
Restoring a Mac from Regular Backups	189
Restoring a Mac from a Replicated Copy	191
What to do if the OS on the new Mac is newer than the backed-up OS	192
Restoring a Windows Client	193
Restoring a Linux Client	193
About Mac OS X's "Recovery HD" partition.....	0
Managing Retrospect	195
Retrospect Preferences	195
Working with Rules	204
Backup Strategies	210
Working with Reports and the Operations Log	215
Managing Media Sets	218
Moving Retrospect	224
Uninstalling Retrospect	225
Troubleshooting and Support Resources	226
Troubleshooting Retrospect	226
Retrospect Support	228
Before you Call Technical Support	228

Appendices

Retrospect Management Console	230
Account Creation	230
System Setup	232
User Creation	235
Organization Creation	236
Overview	146
Script Creation	241

Shared Scripts	244
Compatibility	246
Email Protection	247
Configuration	247
Adding Email Account to Backup Script	248
Performance	249
Remote Data Protection.....	250
VPN Backup	250
Remote Backup	182
Cloud Backup	121
Block Level Incremental Backup	265
Overview	146
Storage Savings.....	265
Usage.....	266
Logging.....	267
Options	267
Backward Compatibility.....	268
Technical Details	149
Instant Scan	270
Legacy Client.....	275
Glossary	288
Release Notes.....	294

What's New

This document contains important information about Retrospect Backup 19 for Mac. Please read it carefully.

The Retrospect website is regularly updated with the most recent support information for Retrospect and related products, including the following:

[Retrospect Support](#)

[Retrospect Updates](#)

[Release Notes](#)

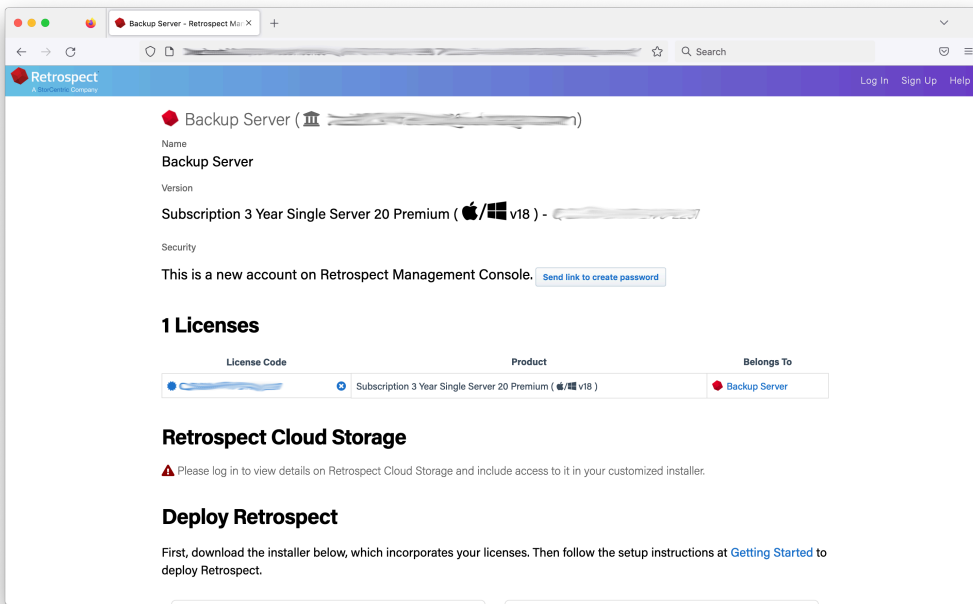
Retrospect Cloud Storage

With Retrospect Backup 19, businesses around the world can now protect their critical infrastructure on Retrospect Cloud Storage, with complete support for immutable backups and anomaly detection, as well as on-premise with Retrospect's deep support for NAS devices and tape libraries.

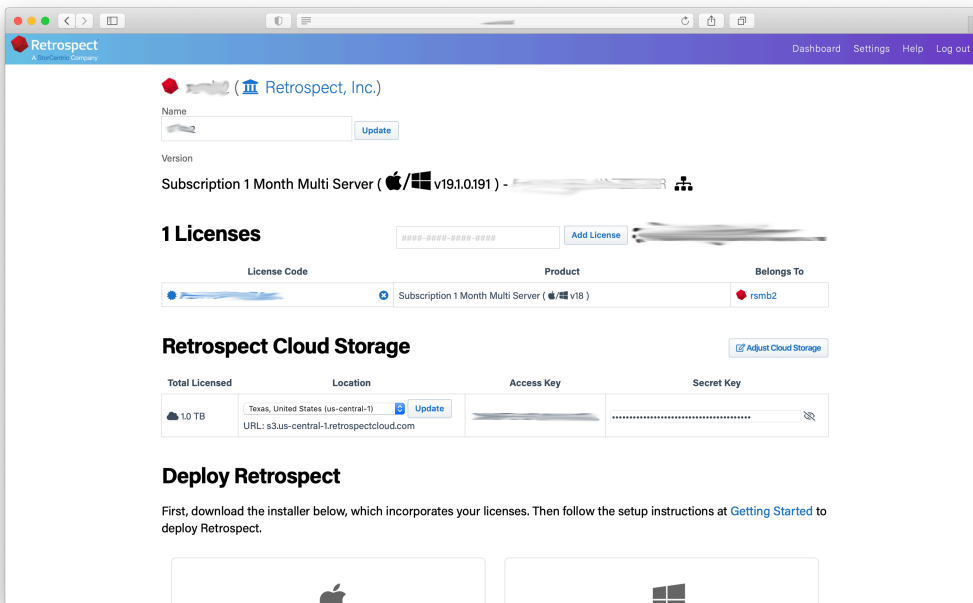
Retrospect Cloud Storage is built on Wasabi Technologies' Hot Cloud Storage, providing lightning-fast object storage. Retrospect Cloud Storage leverages that foundation to provide advanced data protection features like immutable backups. With Retrospect's AES-256 at-rest encryption, sensitive data can be backed up to Retrospect Cloud Storage but guaranteed to remain private from the underlying infrastructure provider, including Retrospect and Wasabi Technologies. Using Retrospect Cloud Storage and the multi-homed backups with the 3-2-1 backup rule, businesses are fully protected and encrypted from ransomware attacks with on-premise and cloud backups.

Retrospect Cloud Storage is available as a subscription license, compatible with both perpetual and subscription licenses. It's available as tiers of 1TB, 5TB, and 10TB.

If you do not have a Retrospect Management Console account and you click on the link for Retrospect 19 with Retrospect Cloud Storage, you'll see a page like this. We allow you to download the Retrospect application with the license included without signing in, but for security, you must create an account and sign in to access Retrospect Cloud Storage.



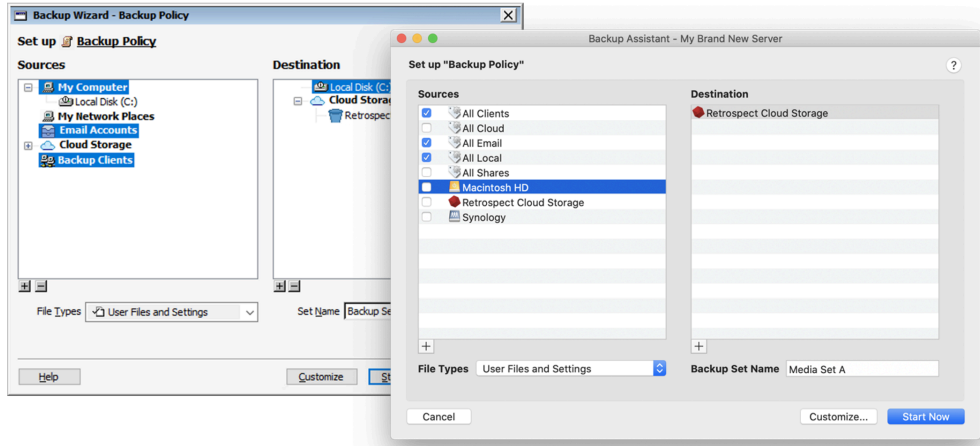
After you sign in, you'll see a page like this.



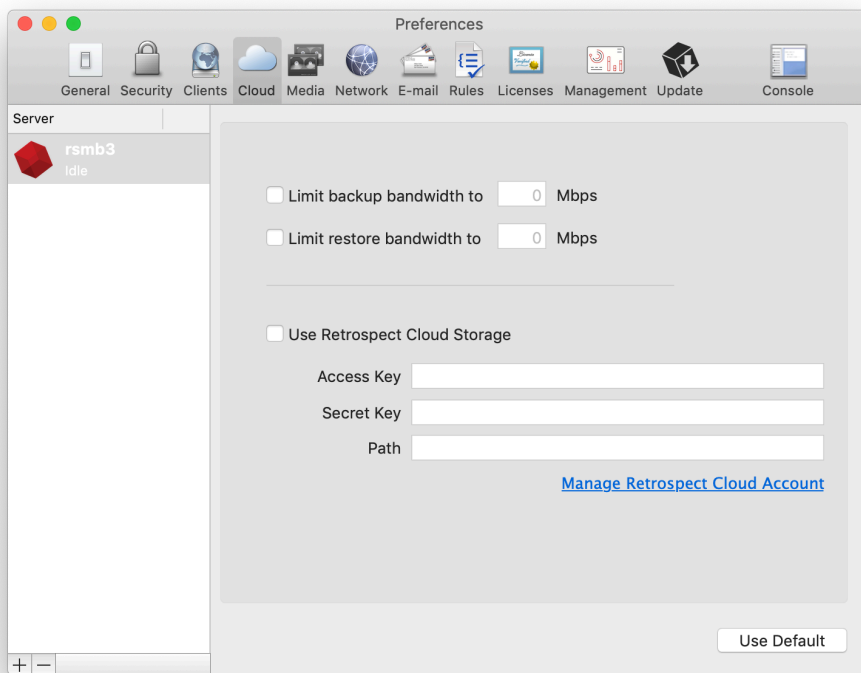
When you download Retrospect from Retrospect Management Console, your license and Retrospect Cloud Storage credentials are included in the personalized configuration file embedded in the download. After you install and launch Retrospect, Retrospect will automatically set up a cloud volume for your Retrospect Cloud Storage account, available in the First Launch wizard.

Retrospect Virtual is fully certified with Retrospect Cloud Storage as well. When you set up a backup set, select "S3-Compatible Storage" and enter the URL, Access Key, and Secret Key from your

Retrospect Management Console engine page.



On Windows and Mac, your Retrospect Cloud Storage information is displayed in Preferences > Cloud.



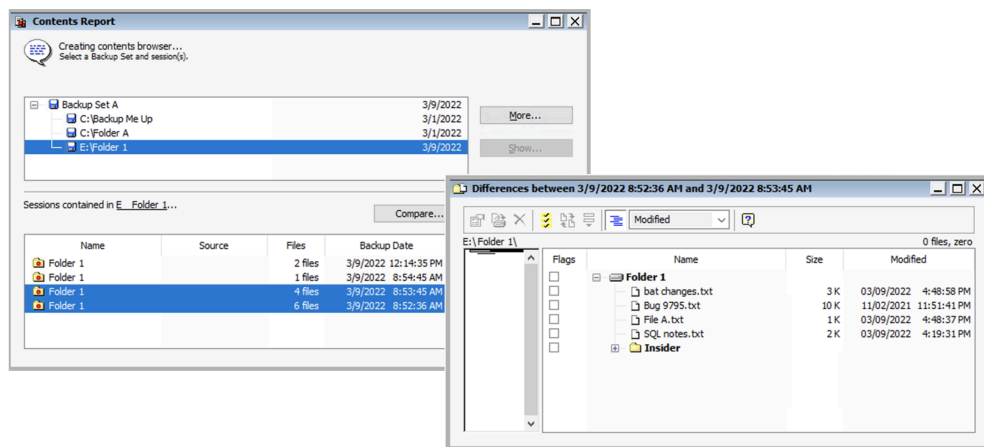
Retrospect Backup 19: Backup Comparison

Businesses need to understand not only what is in a backup but what changed between backups. Using anomaly detection and backup comparison, administrators can identify exactly which files changed to signal an anomaly and evaluate their contents to isolate valid ransomware infections.

If you have a backup that contains more files than you were expecting, backup comparison allows you to drill into exactly which files changed to understand why the backup was bigger.

On Windows: Select a backup set and click "Compare". You can then apply a selector to the results. This is useful if you want to compare backups then use the Anomaly Detection selector to identify which files were detected as anomalies.

On Mac: Select a backup set and click "Compare". Please note that the Mac application is not able to apply a selector to the results.



Retrospect Backup 19: Cloud Performance Improvements

Retrospect Backup 19 includes cloud performance improvements to increase upload speeds to cloud storage providers up to twice as fast. No change is necessary in the script or backup set, and you will see the performance increase on existing backup sets as well as new ones.

Under the hood, Retrospect now supports multi-part upload for compatible cloud providers, including Amazon S3, Microsoft Azure Blob Storage, Backblaze B2 (with S3 API), and Wasabi. Instead of uploading one 600MB RDB file at a time, Retrospect initiates 10 uploads of 5MB chunks of the 600MB RDB file. This approach is able to saturate more of your internet connection as well as recover faster if there is a temporary connection error. These are the settings that optimize upload speeds across the array of situations that we tested, but Retrospect also supports customization of these settings through the INI file.

In addition to internal performance increases, Retrospect continues to be on the leading edge for global cloud storage certifications. The fastest connection speeds will be to local data centers. Please locate the data center nearest you when you use Retrospect for cloud backup.

Retrospect Backup 19: LTO-9 Tape Support

Retrospect Backup 19 now supports LTO-9 tapes with certifications for the latest from HPE, IBM,

Retrospect Backup 19: Multi-Factor Authentication (MFA) and Encryption

Identity protection is important even for on-premise applications. Retrospect Backup will support configuration encryption and multi-factor authentication combined with a password prompt. Even if an attacker gains administrative access to the computer where Retrospect Backup runs, they will not be able to access the program or the configuration files.

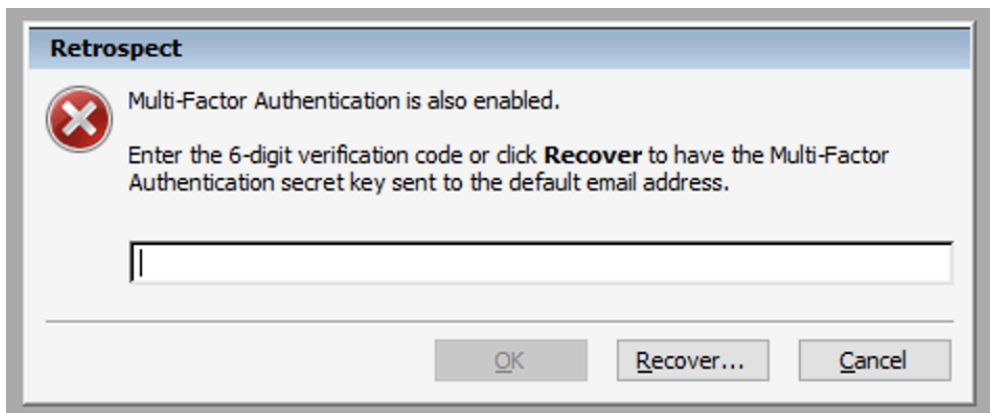
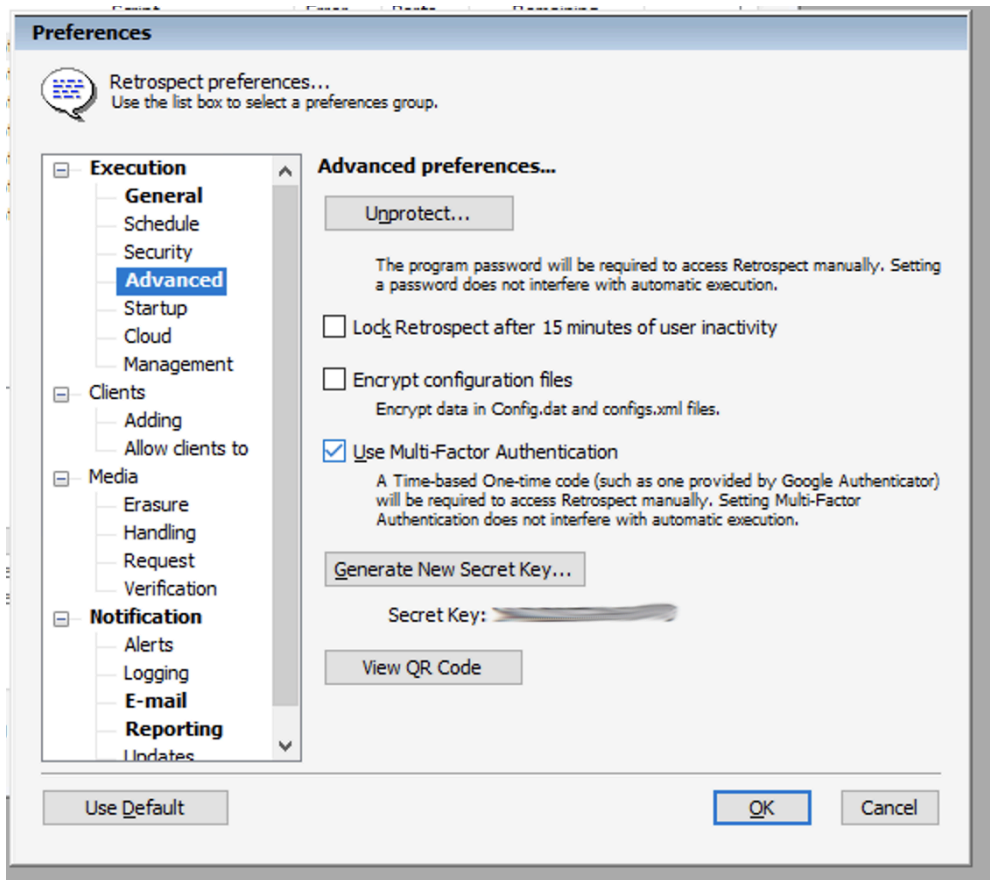
On Windows: In Preferences, select "Advanced". You can select "Encrypt configuration files" (if you have a password configured) and "Use Multi-Factor Authentication". We recommend using the "View QR Code" for adding Retrospect to your MFA mobile app.

On Mac: In Preferences, select "Security". You can select "Encrypt configuration files" (if you have a password configured) and "Use Multi-Factor Authentication". We recommend using the "View QR Code" for adding Retrospect to your MFA mobile app.

When you set up multi-factor authentication and attempt to log in again, Retrospect will ask for your password and the one-time verification code. If you lose your way to generate the one-time codes, Retrospect allows you to click "Recover...", and it will send you an email with the secret key included.

Retrospect's multi-factor authentication is compatible with the leading MFA apps in the App Store, including Duo, Salesforce Authenticator, Google Authenticator, Authy, and Microsoft Authenticator.

NOTE:: Email notifications are required for MFA recovery. If you do not have email set up and you lose the ability to generate the one-time codes, you will lose access to Retrospect.

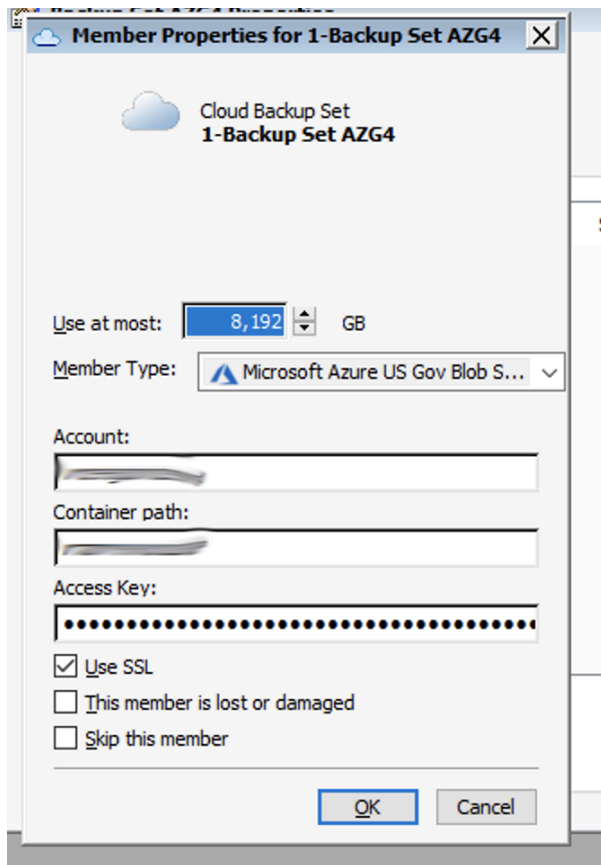


For security, if you are importing a configuration file that had a password and MFA set up, you will need to use the password and one-time code to import it.

Retrospect Backup 19: Support for Microsoft Azure for Government

Retrospect supports blob storage on Microsoft Azure for Government to enhance support for state and local agencies looking for data protection in a US-based high-security data center.

On Windows and Mac, "Microsoft Azure US Gov Blob Storage" is now available in the cloud dropdown menu.



Retrospect Backup 19: Flexible Immutable Retention Periods

Retrospect's ransomware protection allowed customers to completely protect themselves from ransomware using immutable backups stored in their cloud. Retrospect provided an industry-leading workflow with a sliding window of immutable protection. Data in backups that were expiring from the window were again included in the next protected backup, ensuring customers always had a full synthetic backup of every point-in-time backup within that locked window.

However, this workflow does not work for everyone. Other businesses have data that needs to be protected in an immutable backup, but the data does not change often. In the previous workflow, that data was re-backed up whenever it was exiting the sliding window.

Retrospect Backup 19 supports an additional type of retention where Retrospect extends the period on past backups instead of including that data in new backups: "Update retention period for past backups". The archival window option can be applied to a new set or added to an existing set.

Window

Script Clients Share Email >>

Media Set Type: Cloud

Media Set Name: **Media Set B**

Catalog Location: /Library/Applicati...ospect/Catalogs Choose...

Media Set Security: None

Password:
Between 4 and 31 characters

Confirm:

Would you like Retrospect to remember this password?

Remember password for scripted access

Allow Hardware Data Compression

Create as Storage Group

Immutable Retention Policy: days

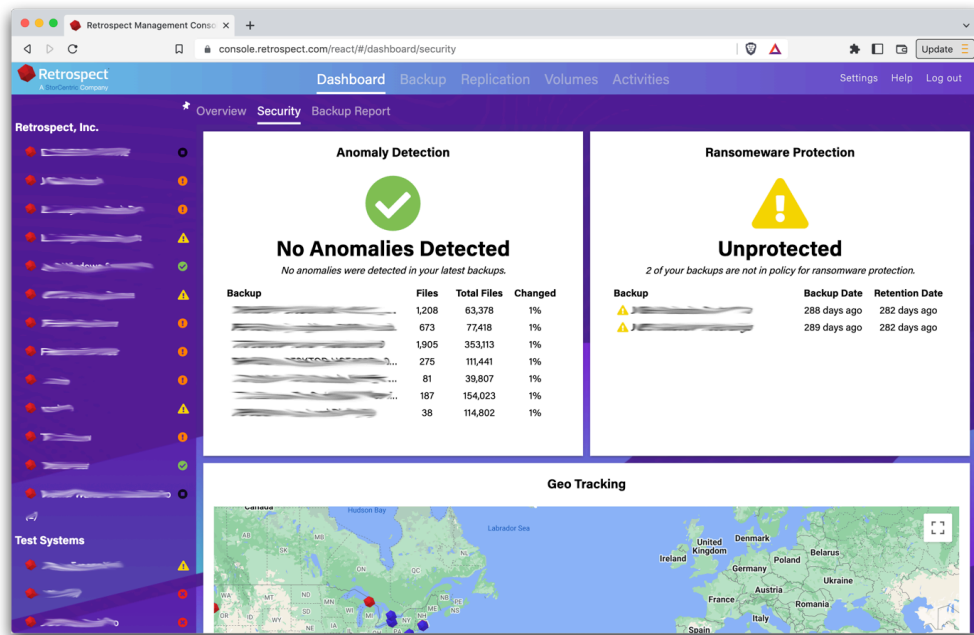
Update retention period for past backups

Cancel Add

backup of each month for the months specified

Retrospect Management Console: Redesigned Dashboard

Retrospect Management Console aggregates your entire infrastructure in a single pane of glass. The most common feedback we received though was that the original dashboard provided too much data. It was so much data that customers found it overwhelming. The redesigned dashboard improves this aggregation to a simple set of graphs to quickly summarize the state of your environment without adding too much detail.

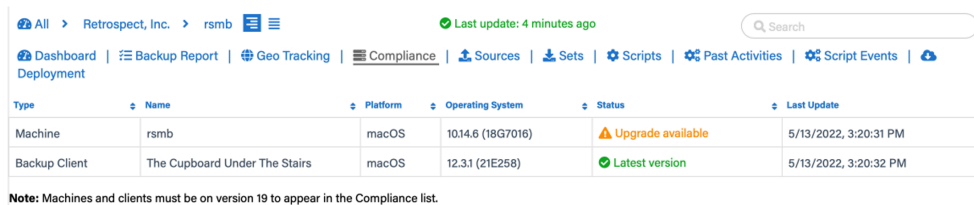


We plan to roll out Redesigned Dashboard for Retrospect Management Console before the official release of Retrospect Backup 19.

Retrospect Management Console: OS Compliance

The most common vector for ransomware is infecting unpatched systems. Keeping systems up to date with the latest OS versions is critical to protecting your infrastructure against ransomware attacks, and now Retrospect makes it easy with OS Compliance. Retrospect Management Console lists all of the systems in your environment with their current OS version and notes whether it's the latest version, enabling you to quickly identify which systems need patching.

If you are not using Retrospect Management Console, no data is sent to Retrospect. If you are using Retrospect Management Console, the OS information is automatically included with the rest of the backup data sent.



Retrospect Management Console: Multi-Factor Authentication

Retrospect Management Console now supports Multi-Factor Authentication.

Retrospect Management Console: Audit Log

Retrospect Management Console now supports an Audit Log for tracking changes within your account.

Bug Fixes

This latest release of Retrospect includes fixes for numerous issues. For a list of bugs fixed in this release, please refer to the [Release Notes](#).

Quick Start Guide

Retrospect Backup is a powerful data protection suite with a multitude of features. Before we dive into the details, let's walk through a simple example of using Retrospect Backup to protect a Word document on your desktop.

First Launch Experience

Retrospect Backup has been protecting data at homes and businesses since 1989. Getting a first backup can mean the difference between success and failure as a business, and Retrospect Backup has a simple workflow to simplify that experience while making it easier for new users to see what will be backed up.

Default first launch backup wizard

The screenshot shows the 'Backup Assistant - JG's MacBook Pro' window. It has two main panes: 'Sources' and 'Destination'. The 'Sources' pane has checkboxes for 'Local volumes', 'Macintosh HD', 'Other computers', 'Email accounts', 'Cloud volumes', and 'Network volumes'. The 'Destination' pane has a list with 'Macintosh HD', 'Public', and 'Synology'. Below these panes is a 'File Types' dropdown set to 'User Files and Settings' and a 'Backup Set Name' field containing 'Backup Set A'. At the bottom are 'Cancel', 'Change options or schedule', 'Customize...', and 'Finish' buttons.

Annotations:

- Default script name, can be changed later (points to the window title)
- Backup all local drives, any client computers and any Email (points to the Sources list)
- Add email, cloud, NAS or other computers (See next slides) (points to the Sources list)
- Default selector for all User data (points to the File Types dropdown)
- Change options or schedule (points to the Customize... button)
- Preselects first reasonable destination (points to the Public destination)
- To add Cloud or NAS destination (points to the Synology destination)
- Default unique name (points to the Backup Set Name field)
- 80% of our users can just click "Finish" (points to the Finish button)

Adding Other Computers (Clients)

The 'Other Computers' version of the gallery is used to direct them to the management console.

The dialog box has a title bar 'Add: Other Computer'. Below it is a text area with the following content:

Retrospect can back up other computers on your network using the Retrospect Client software. On the computer you wish to back up, open the following link:

https://console.retrospect.com/machines/874595238/client_installers

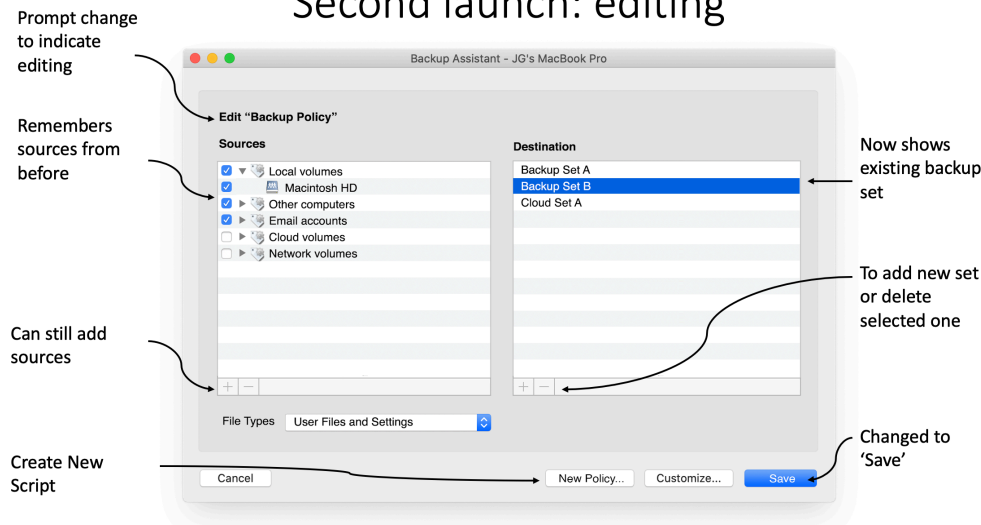
This will download a single-click application that will install the Retrospect Client software. Once installed, it will automatically be added to this Retrospect backup server and be available for backup.

At the bottom are 'Cancel' and 'Add' buttons.

Annotation:

- Installer can also be deployed via Munki, Desktop Central and other external platforms (points to the URL)

Second launch: editing



The backup wizard starts with a single screen, showing sources and destinations with a default backup selector. Finish with a single click or add new data sources or destinations. With deep integration with Retrospect Management Console, Retrospect Backup makes it easy to send a single download link to an entire company for everyone to download the Retrospect Backup agent, install it with a single click, and let Retrospect Backup take care of the rest.

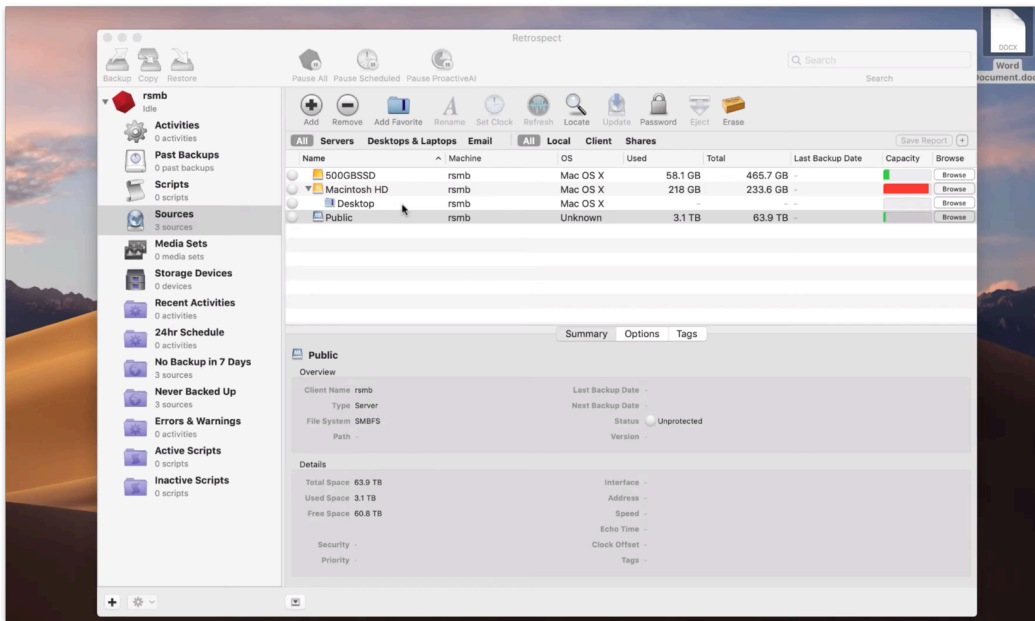
Under the hood, Retrospect Backup includes new features like 10x faster automated generation for public/private keypairs with seamless upload to Retrospect Management Console and embedded unique trial licenses to remove any barriers to getting that first backup.

Backup

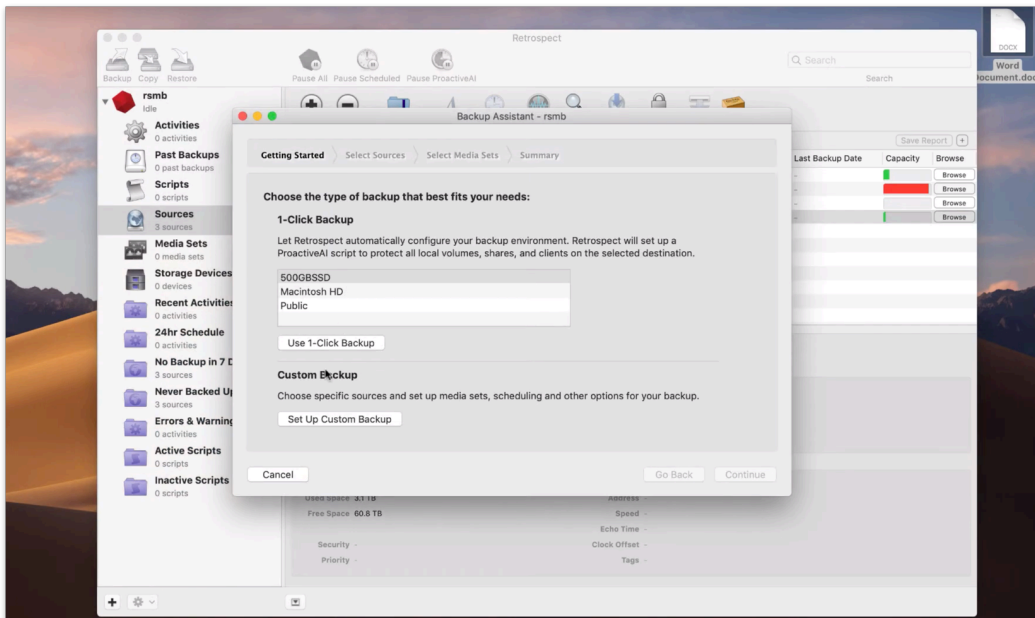
We are going to back up the Word document, and then we are going to restore it.

You see the Word document at the top right of the screen on the Desktop. Let's back up the Word document using Backup Assistant. The Backup Assistant is how you set up your backup strategy using sources (volumes and clients), media sets (destinations for your backups), and scripts (the backup plan for your sources and sets).

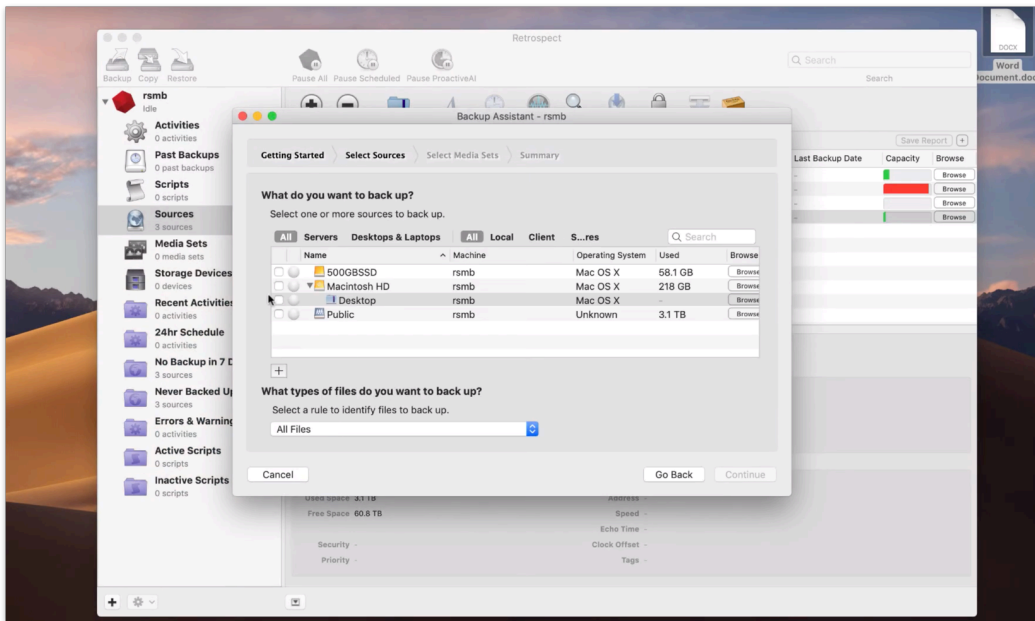
Launch the Backup Assistant by clicking "Backup" at the top left of the screen in Retrospect.



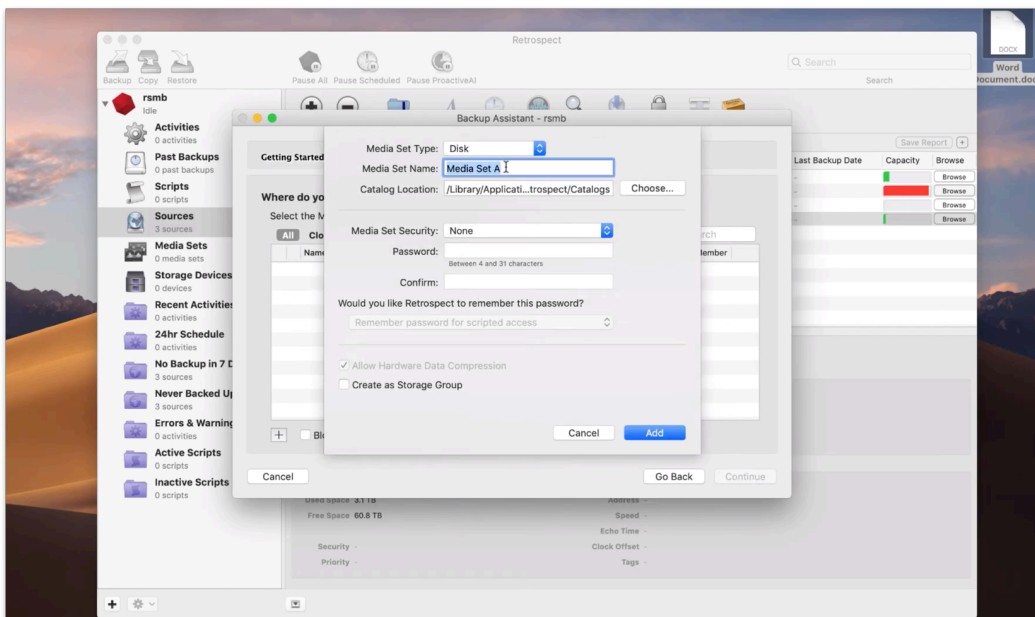
In Backup Assistant, select "Set up Custom Backup".



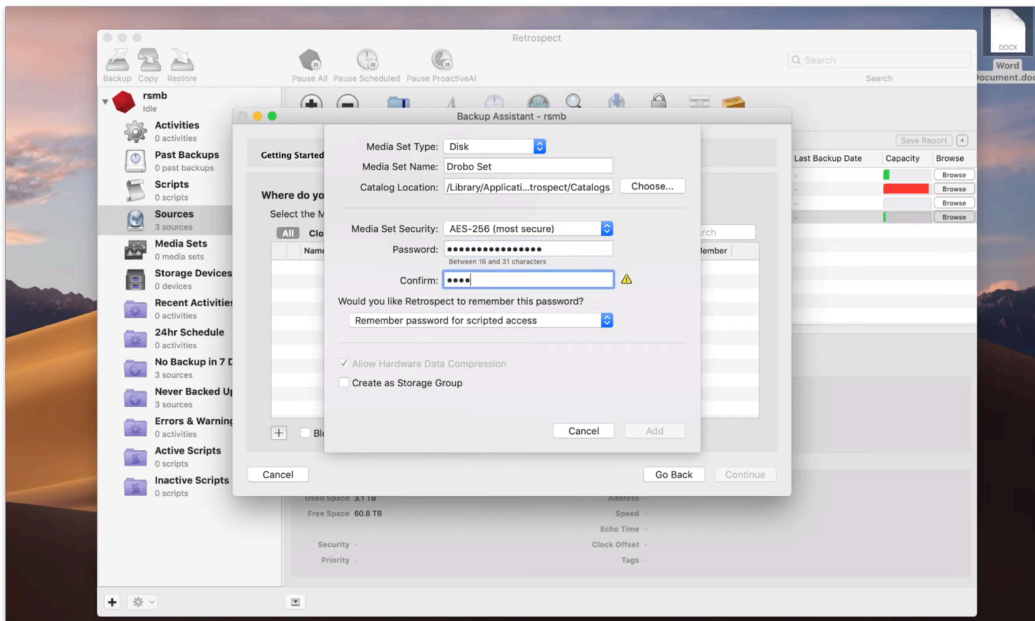
To back up only the Desktop, we need to create a favorite folder. Click "Browse" on "Macintosh HD", browse to your Desktop under `/Users/your_name/Desktop` and click "Add as Favorite Folder". Then select "Desktop" in Backup Assistant.



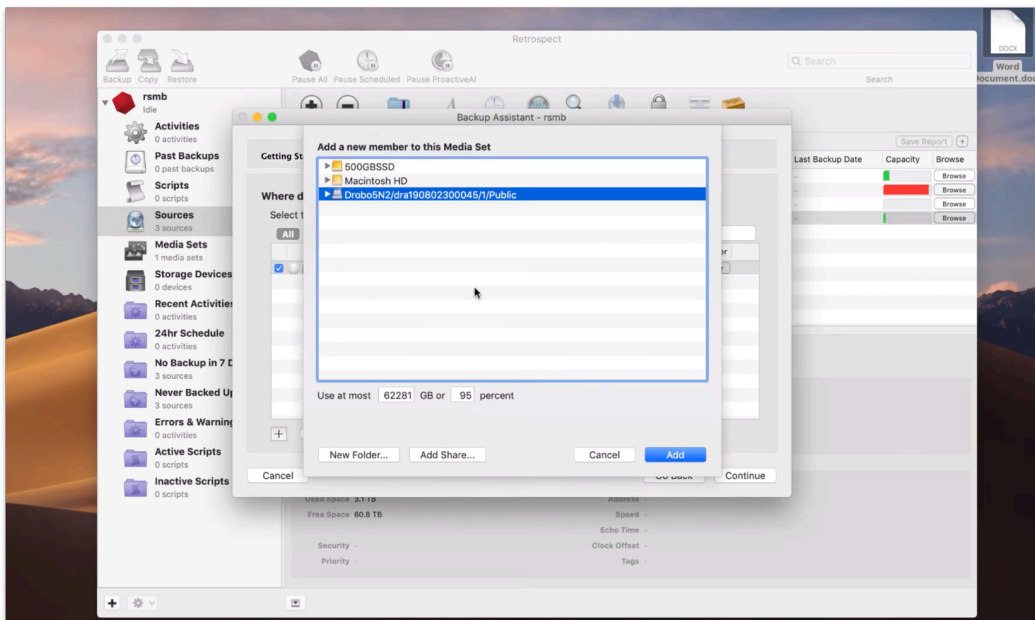
Next, we need to create a destination for the backup to be stored on, called a media set (or a backup set). Click the "+" icon at the bottom to create a new media set. We are going to use "Disk", but you can also use "Cloud" or "Tape" as a destination. Type in a media set name.



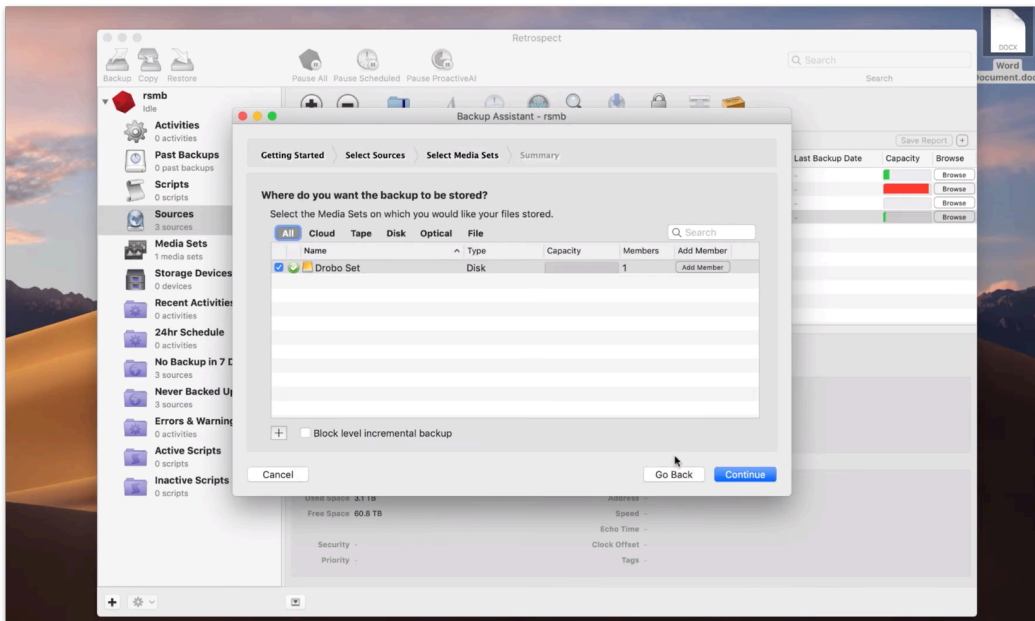
Retrospect supports many types of encryption, including AES-256, to ensure only you can read your backups, even if you store your backups in the cloud. Select "AES-256" and type in a password. Please write down your password. If you lose it, your data will not be recoverable by anyone.



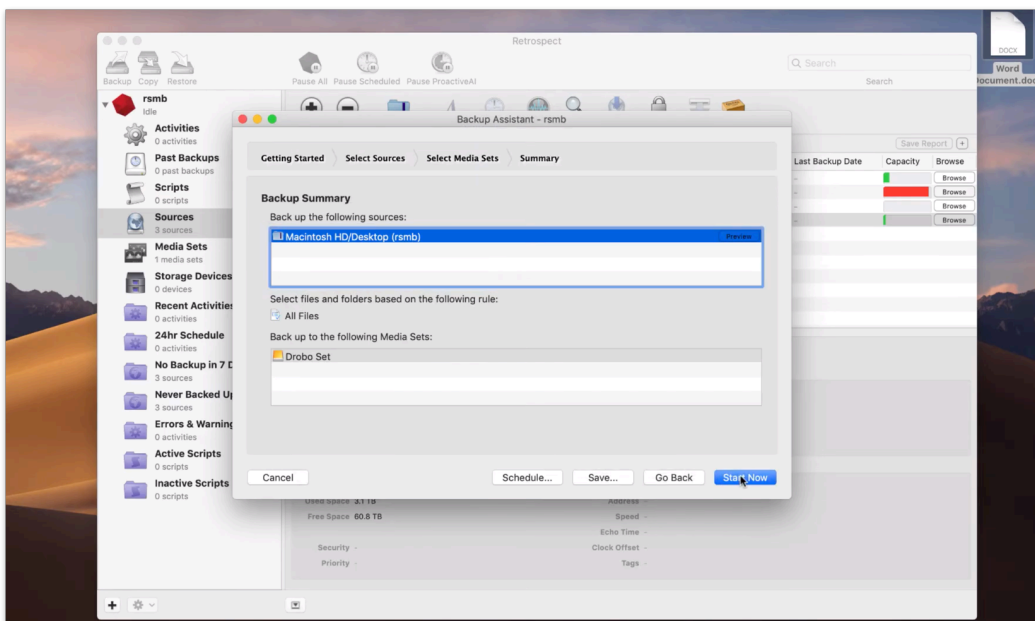
We are going to select a NAS share, but you should select the appropriate destination, be it an external hard drive or a NAS. Click "Add".



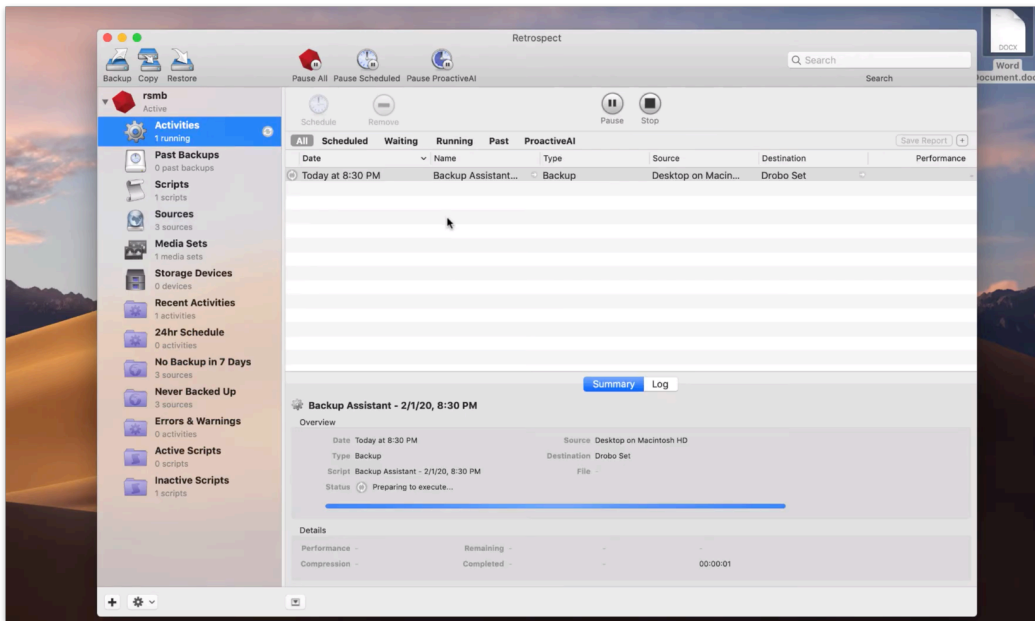
The media set is created. Select it and then click "Continue".



Backup Assistant is done. You can see the summary here. Click "Start Now" to start the backup.



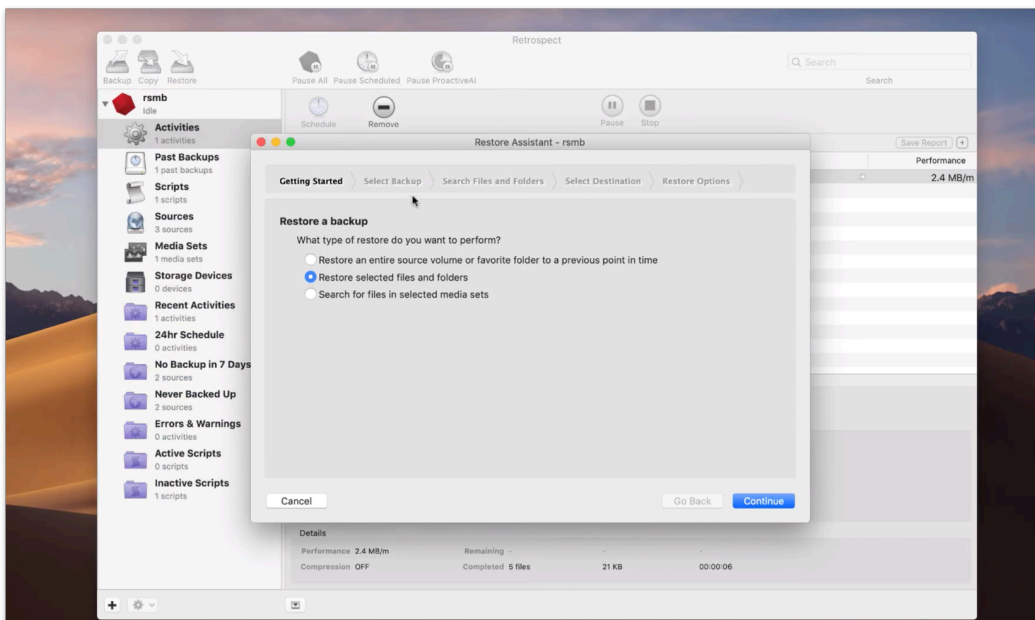
The backup is now running. Your Word document is being safely protected on the destination you chose.



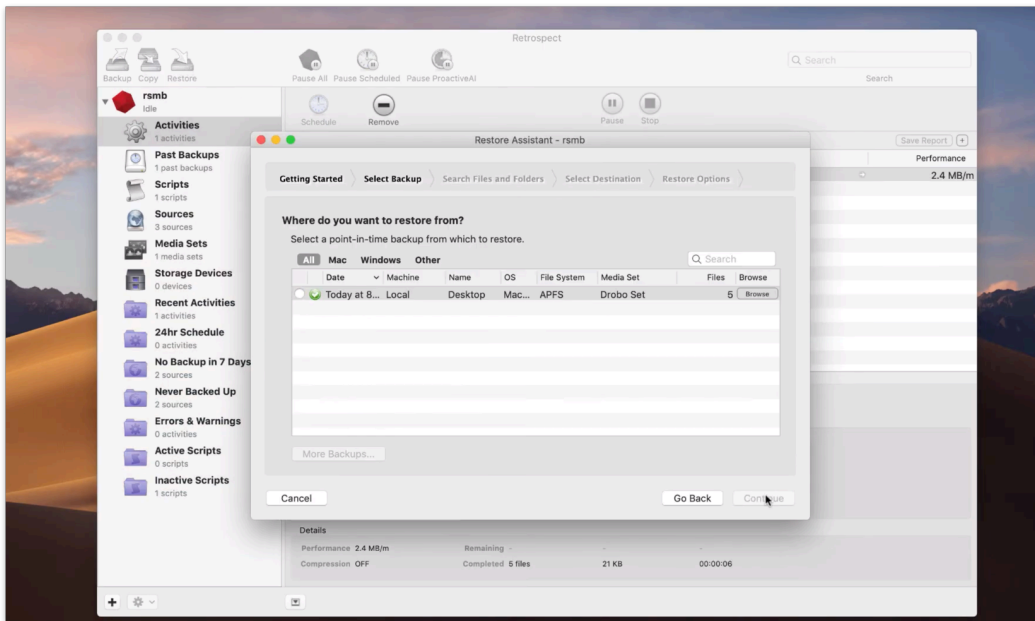
Restore

Let's now delete the Word document from the Desktop and restore it with Retrospect.

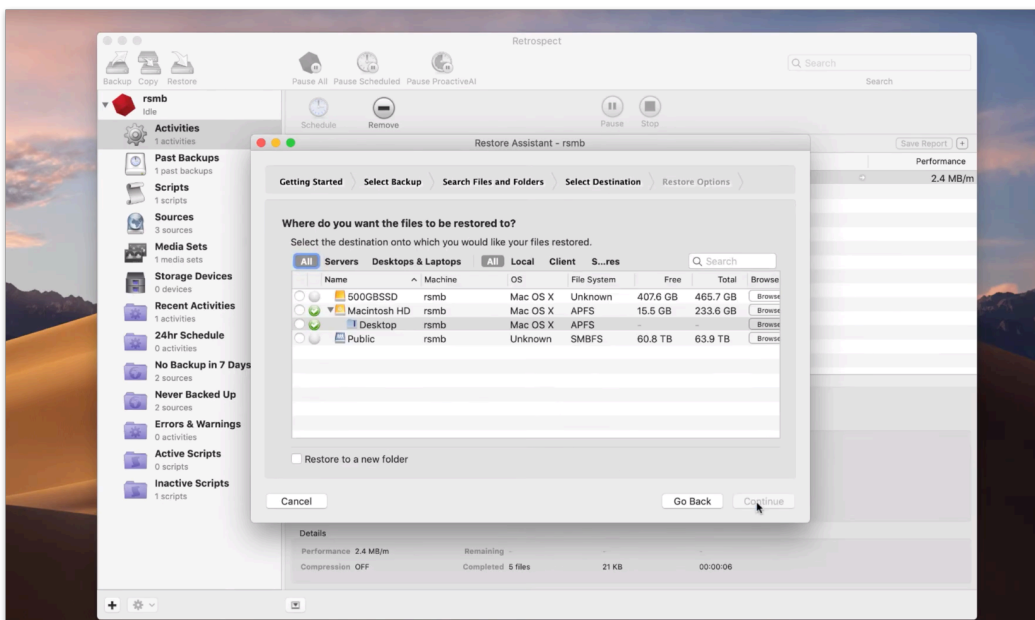
Launch Restore Assistant by clicking "Restore" in the top left corner of Retrospect. Click "Restore selected files and folders".



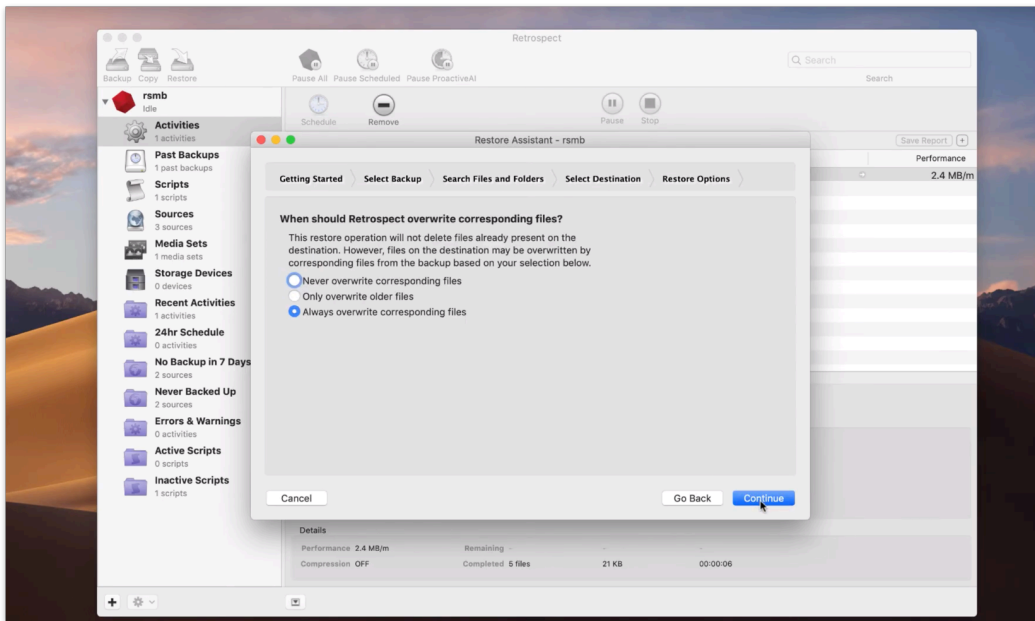
Select the latest backup and click "Continue".



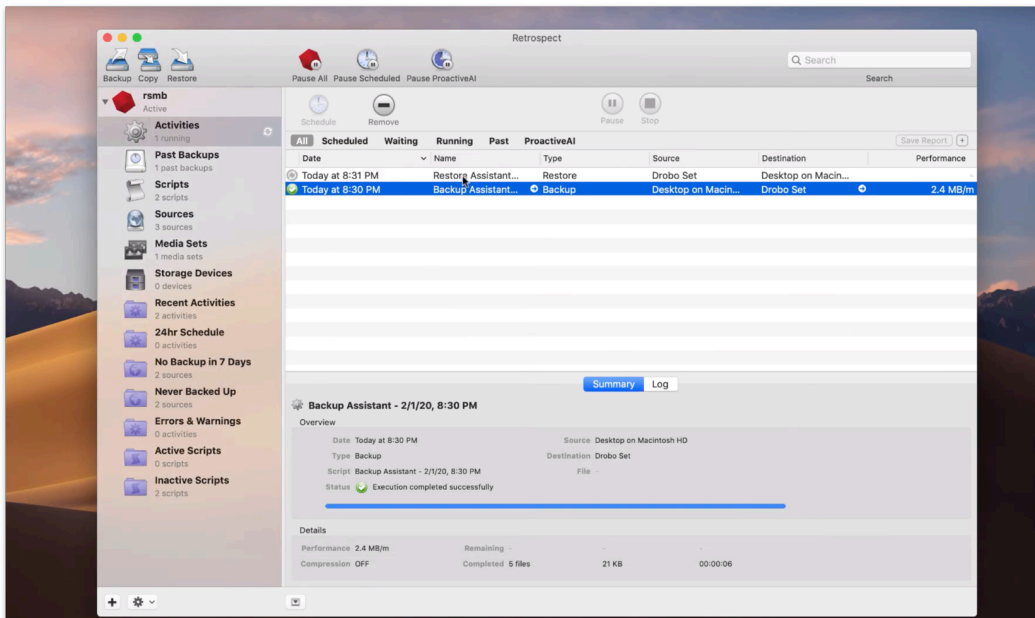
Now you need to choose where to restore the backup to. Select "Desktop" to restore the desktop files, including the Word document, back to where they were.



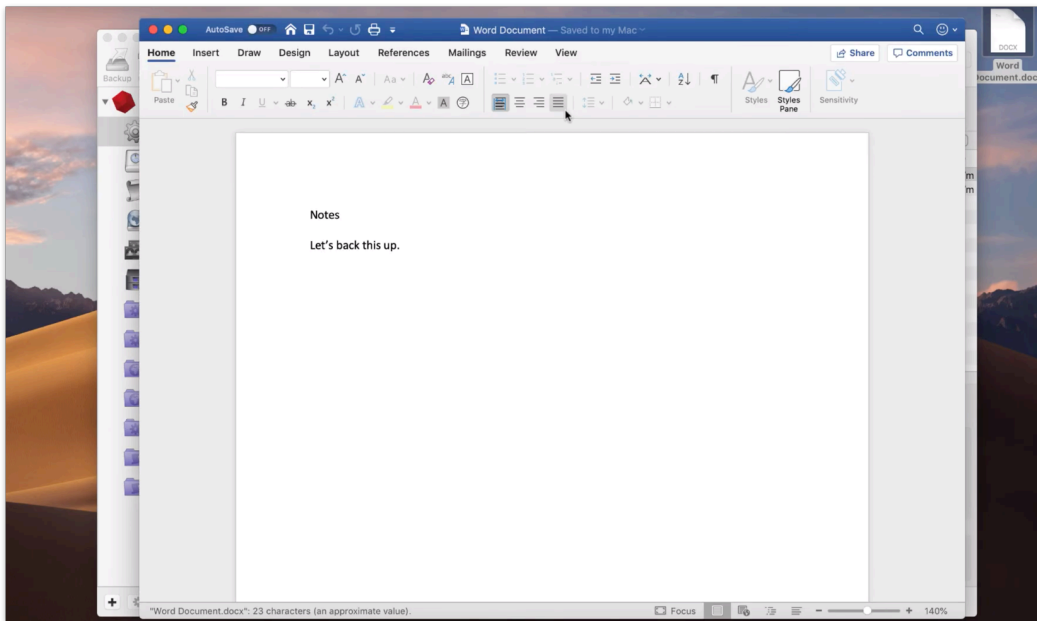
Retrospect offers granular restore options. For this scenario, we select "Always overwrite corresponding files". Click "Continue" and then click "Restore".



The restore is now running.



Our Word document is back on the Desktop.



Introducing Retrospect

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:

Multi Server – Protects any number of networked Windows, Mac, and Linux servers, desktops, and notebooks from a single host computer running Retrospect. Supports disk, cloud, and tape storage devices.

Single Server Unlimited – Protects one server and any number of networked Windows, Mac, and Linux desktops and notebooks from a single host computer running Retrospect. Additional server client licenses can be purchased to protect more networked Windows, Mac, or Linux servers. Supports disk, cloud, and tape storage devices.

Single Server 20 – Protects one server and up to 20 networked Windows, Mac, and Linux desktops and notebooks from a single host computer running Retrospect. Additional Retrospect Client and server client licenses can be purchased to protect more systems. Supports disk, cloud, and tape storage devices.

Single Server 5 – Protects a single Mac Server and five workstations using local, network, and cloud disk-based storage. Tape devices are not supported.

Desktop – Protects a single non-server Mac and up to five additional Windows, Mac, and Linux desktops and notebooks.

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.

Open File Backup Unlimited – Protects open files on NTFS-formatted volumes on Windows servers, desktops, and laptops. This add-on makes it possible to protect line-of-business applications—such as accounting, CRM, and proprietary database systems—while they’re running, even those with data files spread across multiple volumes. Retrospect’s Open File Backup Unlimited add-on extends to all Windows systems protected by your Retrospect host server, including end-user desktops and laptops.

Advanced Tape Support – Improves backup times by utilizing multiple tape drives in parallel, including multiple stand-alone drives, drives in libraries, or drives in autoloaders. The Advanced Tape Support add-on is licensed per Retrospect host server, not per tape drive. For example, only one Advanced Tape Support add-on license is required for a library with four tape drive mechanisms.

Retrospect Client Packs – Extends the number of networked desktops and notebook computers that can be backed up using Retrospect Disk-to-Disk or Desktop editions. Available in 1, 5, and 10 client license packs.

Retrospect Server Client – Extends the number of networked servers that can be backed up using Retrospect Single Server editions. Each Retrospect Server Client adds a license for protecting one additional server as a network client.

Annual Support & Maintenance (ASM) – Provides technical support via email and phone (available in select regions) and all upgrades/updates of purchased product at no additional cost for 1 year from the date of ASM purchase.

System Requirements

Retrospect Backup 19 for Mac

Supported Operating Systems:

Apple macOS Sonoma / Sonoma Server 14

Apple macOS Ventura / Ventura Server 13

Apple macOS Monterey / Monterey Server 12

Apple macOS Big Sur / Big Sur Server 11

Apple macOS Catalina / Catalina Server 10.15

Apple macOS Mojave / Mojave Server 10.14

Apple macOS High Sierra / High Sierra Server 10.13

Apple macOS Sierra / Sierra Server 10.12

Apple OS X El Capitan / El Capitan Server 10.11.6
Apple OS X Yosemite / Yosemite Server 10.10.5
Apple OS X Mavericks / Mavericks Server 10.9.5
Apple OS X Mountain Lion / Mountain Lion Server 10.8.5

* Retrospect Desktop doesn't run on Mac OS X Server.

Supported Hardware:

Apple Silicon processor with one or more multicore processors
Intel processor with one or more multicore processors

Recommended Configuration:

Latest Software Update for OS X
1 GB for each concurrent activity; 4 GB minimum
10–15 GB of temp hard disk space for each concurrent activity (backup, restore, etc.)
Adequate storage for backups
RAM that meets Apple's guidelines for each OS

Retrospect Backup 19 Client for Mac

Apple macOS Sonoma / Sonoma Server 14
Apple macOS Ventura / Ventura Server 13
Apple macOS Monterey / Monterey Server 12
Apple macOS Big Sur / Big Sur Server 11
Apple macOS Catalina / Catalina Server 10.15
Apple macOS Mojave / Mojave Server 10.14
Apple macOS High Sierra / High Sierra Server 10.13
Apple macOS Sierra / Sierra Server 10.12
Apple OS X El Capitan / El Capitan Server 10.11.6
Apple OS X Yosemite / Yosemite Server 10.10.5
Apple OS X Mavericks / Mavericks Server 10.9.5
Apple OS X Mountain Lion / Mountain Lion Server 10.8.5

* Backing up server OS clients requires Retrospect Multi Server or other Server edition with available Server Client Licenses.

Supported Hardware:

Apple Silicon processor with one or more multicore processors
Intel processor with one or more multicore processors

Recommended Configuration:

Latest Software Update for OS X
RAM that meets Apple's guidelines for each OS

Retrospect Backup 19 Client for Windows

Microsoft Windows 10 and 11
Microsoft Windows XP, Vista, 7, 8
Microsoft Windows Server 2003, 2008, 2012, 2012 R2, 2016, 2019, 2022

Microsoft Windows Server Core 2008 R2, 2012, 2016, 2019
Microsoft Windows Server Essentials 2012, 2016
Microsoft Windows SBS 2003, 2008, 2011
Microsoft Windows Storage Server 2003, 2008

*Backing up server OS clients requires Retrospect Multi Server or other Server edition with available Server Client Licenses.

Retrospect Backup 19 Client for Linux

x86- or x64-based system running Red Hat Linux, Red Hat Enterprise Linux, CentOS, Debian, Ubuntu Server and SUSE Linux ([Details](#))
glibc version 2 or later

Storage Devices

Retrospect supports a wide variety of storage devices as the destination for backups, including hard drives (both direct- and network-attached), tape drives and libraries, flash storage, and removable disk drives (RDX, REV, etc.). See the [Retrospect Device Support Database](#) for a complete list of supported tape drives and libraries.

Installing Retrospect Backup

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.

Installing the Retrospect Backup Console and Retrospect Backup Engine

To install the Retrospect console:

Download Retrospect Backup for Mac from the website.

Unzip the file.

Double-click on "Install Retrospect".

Click "Install Retrospect" from the dialog.

Retrospect Backup Console will be installed in "Applications" and auto-launched, and Retrospect Backup Engine will be automatically installed and launched in the background as a service.

For macOS Mojave and macOS Catalina, please follow our step-by-step guide for enabling "Full

Disk Access" below. See the [step-by-step guide](#).

If you need Retrospect Backup Console without an engine installed, please visit our Downloads page.

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.

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.

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.

When prompted by the Installer, enter an administrator's username and password, then click OK.

Follow the installer program's instructions.

For macOS Mojave and macOS Catalina, please follow our [step-by-step guide](#) for enabling "Full Disk Access" below. See the [step-by-step guide](#).

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

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.

Enter the following commands.

```
$ tar -xf Linux_Client.tar
$ ./Install.sh
```

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 for Mac has a different underlying architecture and uses different configuration files than previous versions of Retrospect for Mac, version does not import settings from version 6.x or earlier installations. When upgrading, it is therefore necessary to rebuild the backup environment in Retrospect. 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 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).

Upgrading from Retrospect 6.1

The Retrospect for Mac installation process does not overwrite or remove existing Retrospect 6.1 (or earlier) installations. It is recommended that you continue to maintain your existing Retrospect installation until you are comfortable with Retrospect for Mac.

To keep your existing Retrospect 6.1 (or earlier) installation and prevent that version's scripts from automatically running, take the following steps:

For each backup, duplicate, and restore script with a schedule, edit the script's schedule and check the box to "Skip scheduled executions." Enter a date that is several years in the future.

For each Backup Server script, edit its schedule and set the schedule to never active.

Should you instead wish to remove your previous installation of Retrospect, locate the disk image

containing the installer for your current Retrospect installation (or download it from the Archives section of the Retrospect website) and follow these steps:

Double-click the Install Retrospect icon and provide your password and agreement to the license.

Choose Uninstall from the Easy Install pop-up menu.

Click the Uninstall button and follow the on-screen instructions.

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.

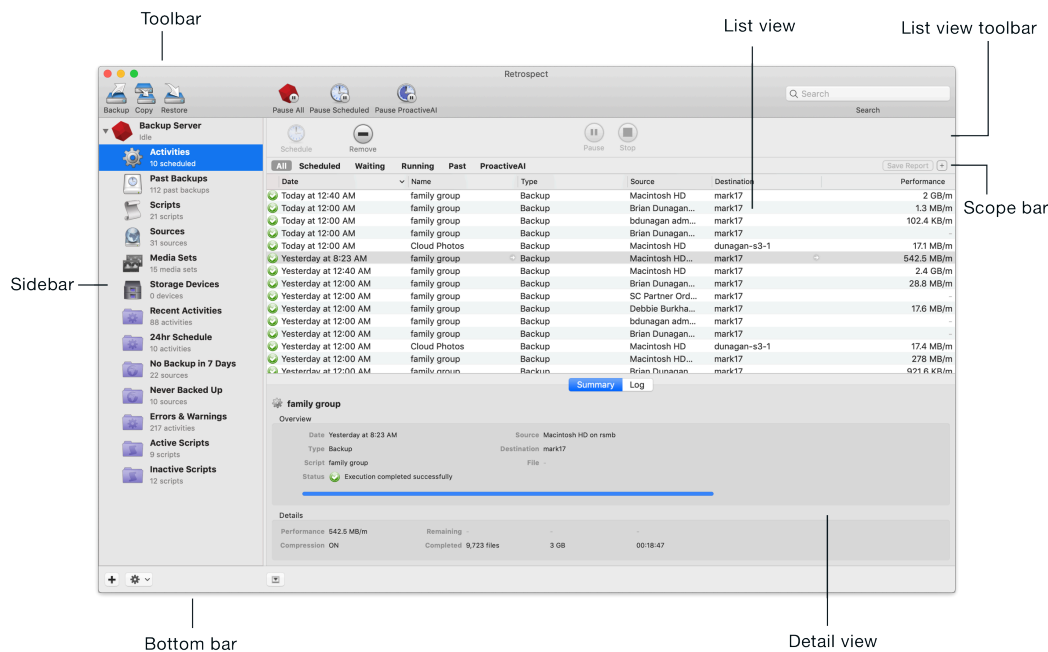
You should also assign a password for each Retrospect engine you logged in by clicking the "Change server password" button and entering a password of your choice. This step prevents unauthorized access of the Retrospect engine from other Retrospect console applications running on your network.

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 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 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.

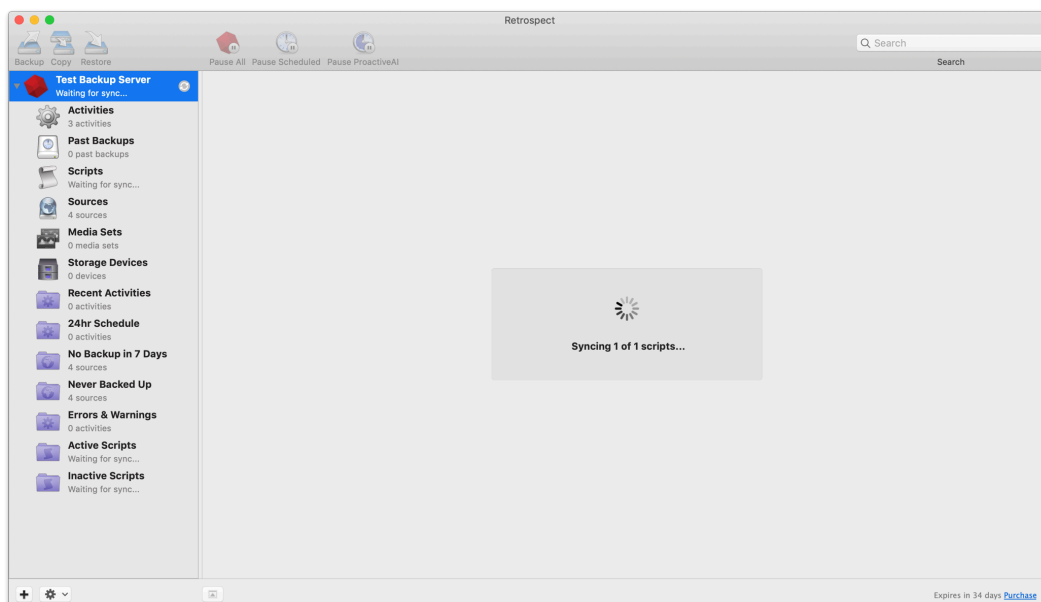
Bottom Bar

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.

Other Views

First Launch — When the Retrospect console first launches it displays the startup view. From here you can install a local server, add a remote server, view this User's Guide, contact Support, and visit the Retrospect website.

Syncing Server — When the Retrospect console connects to a server, it will sync that server's information. For small installations, this process is quick, but for larger ones, this may take a while. The console is optimized to let you get started while the syncing process is running in the background.



Multiple Servers — Retrospect can control multiple servers from the console window. A separate Retrospect license is required for each server. There is full support for Mac version 9.0 and above and limited support for Mac version 8.2.

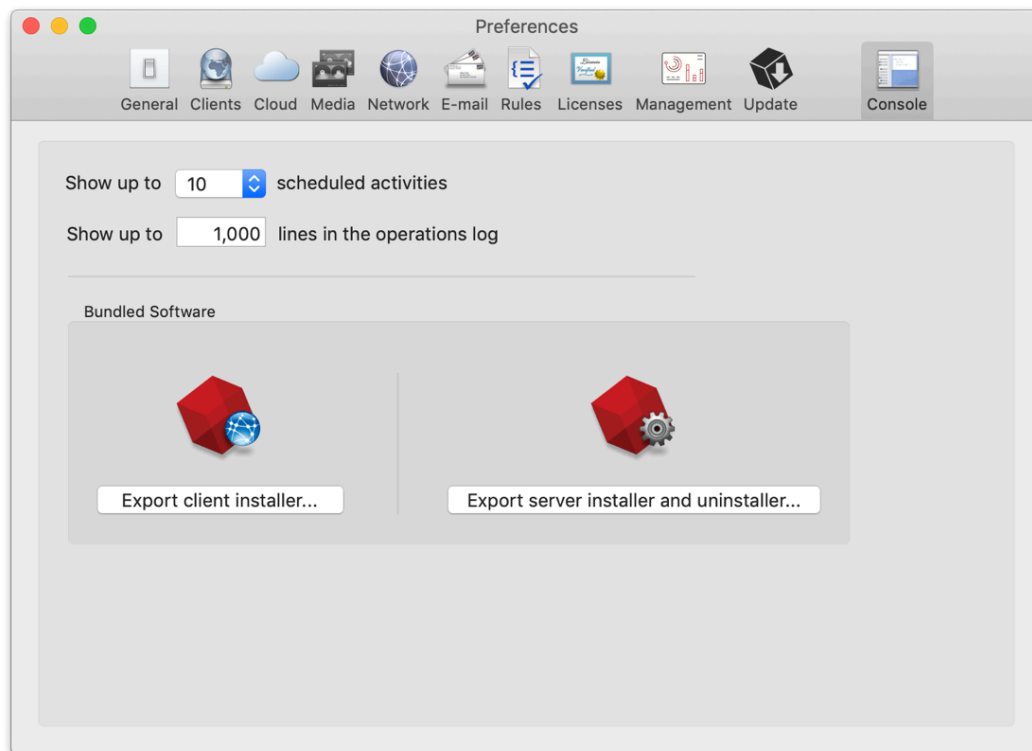
Licensing Server — When adding a server, Retrospect will prompt you to enter your license code. Enter the license code then click Add.

Unlocking Server — When adding a server that has a password Retrospect will display a password error and let you update the password.

Updating Server — Each new version of the Retrospect console includes an updated server installer. When the console is launched it will notify you if your servers can be updated. If you choose not to install the updated server, you can do so at any time.

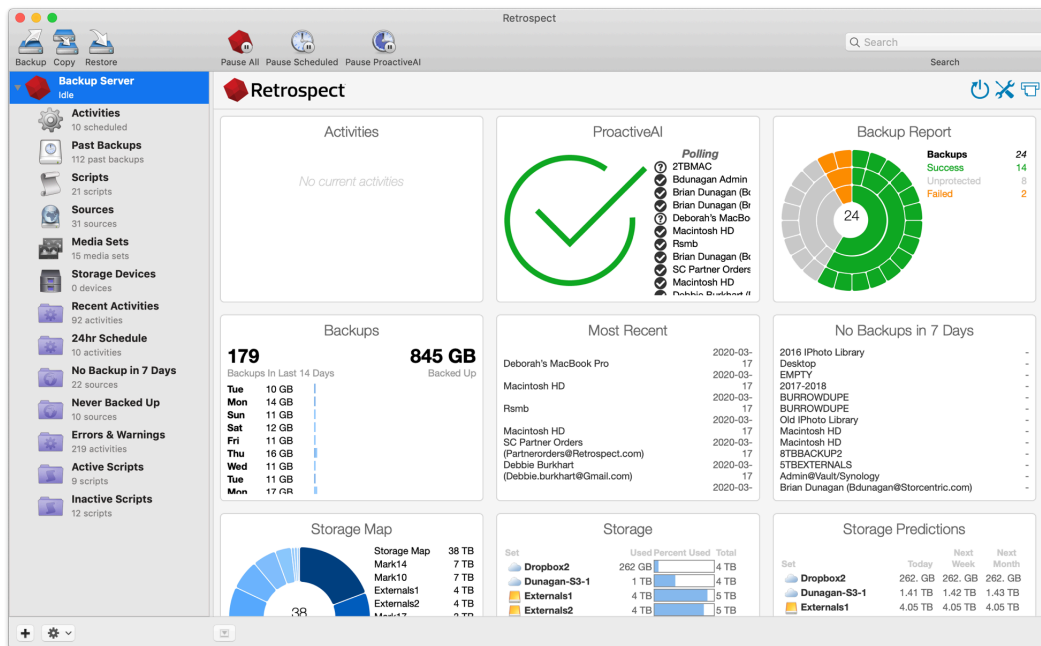
Updating Server — To install the updated server at a later time, click the update icon. Retrospect will automatically install the new server software.

Exporting Installers — Retrospect includes a server installer, client installers for Mac, Windows, and Linux, and client updaters (RCUs) for Mac, Windows, and Linux. To export these to a local folder, open *Preferences* from the menu bar under *Retrospect > Preferences...* and click on *Console*.



Retrospect Dashboard

Retrospect Dashboard gives you a detailed monitoring view for your entire Retrospect Backup engine. Let's walk through each section of the dashboard to discuss how you can use it to understand the current status of your business's data protection strategy.



Activities

Running activities are displayed here.

ProactiveAI

You can see which sources are protected or not protected with ProactiveAI and their respective statuses. It should be all green, unless you have a subset of sources protected by scheduled scripts.

Backup Report

You can see all of the sources within the scope of your search and their statuses:

Green: This is a source with a successful backup.

Orange: This is a source with a failed backup.

Black: This is a source with a stopped backup.

Gray: This is an unprotected source.

This coloring gives you an at-a-glance check for how your backups are doing. If they are not all green, you should drill into which ones are not fully protected.

Backups

This is a list of the backups within the last 14 days and how much data they backed up.

Most Recent

This is a list of the most recently protected sources and the date they were last protected.

No Backups in 7 Days

This is a list of sources that have had no backup in 7 days.

Storage Map

You can see how much data each backup set takes up and the total amount used.

Storage

This is a list of the backup sets and their usage.

Storage Predictions

Storage Predictions takes the current analytics for each set and predicts how much data will likely be used in the next week and the next month. You can use this to estimate when to add more storage or when Retrospect grooming will occur to free up space.

Enabling "Full Disk Access"

macOS Catalina (10.15) extends the Full Disk Access security feature from macOS Mojave (10.14) to help users manage their data privacy. This additional protection ensures you know exactly which applications have access to your data by requiring explicit consent for file-level access to certain application data folders, like Mail, Messages, and Safari, so Retrospect Backup engine and client will not be able to access the entire system without explicit user action. Follow our step-by-step guide to allow Retrospect Backup to continue protecting your Mac environment, under System Preferences > Security & Privacy > Privacy > Full Disk Access.

Engine Setup

Open "System Preferences" under the Apple at the top left of your screen.

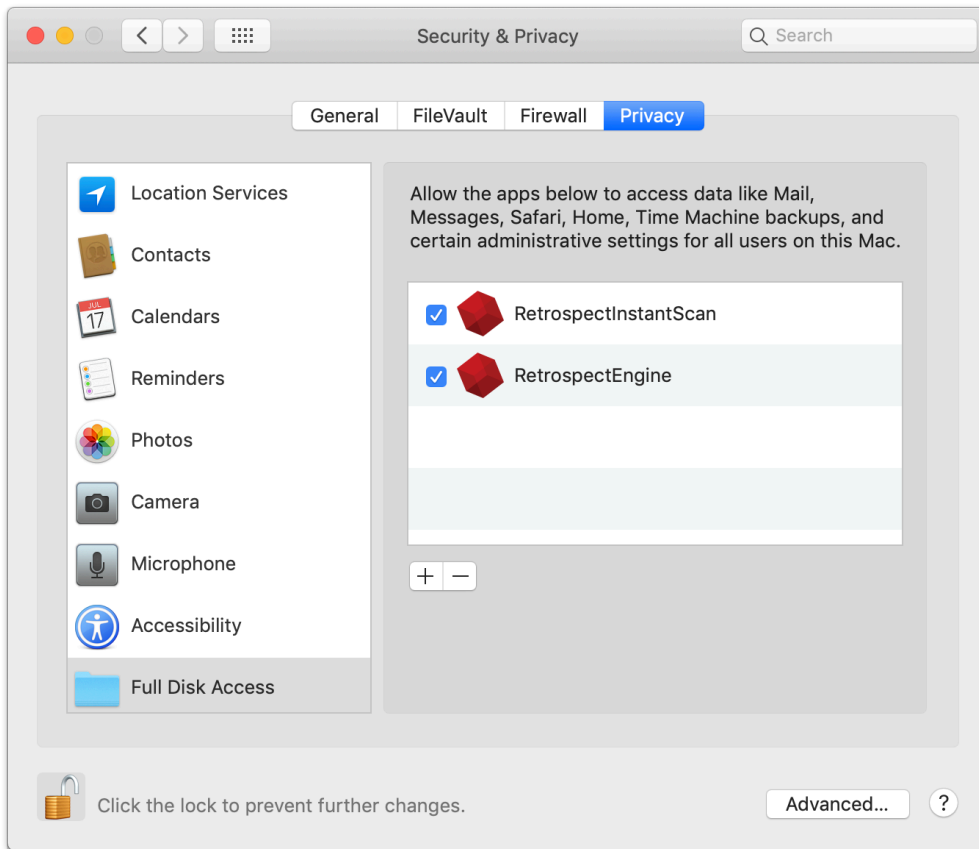
Click on "Security & Privacy" then "Privacy". You should see "Full Disk Access".

Click on the lock to authenticate and allow changes.

Now you need to find the Retrospect applications to drag into this list. Go to "Finder". Select "Go" from the menu bar and then "Go to Folder...". Enter:

```
/Library/Application Support/Retrospect
```

Scroll down "RetrospectEngine" and "RetrospectInstantScan" and drag them into the "Full Disk Access" list. Close "System Preferences".



Client Setup

Open "System Preferences" under the Apple at the top left of your screen.

Click on "Security & Privacy" then "Privacy". You should see "Full Disk Access".

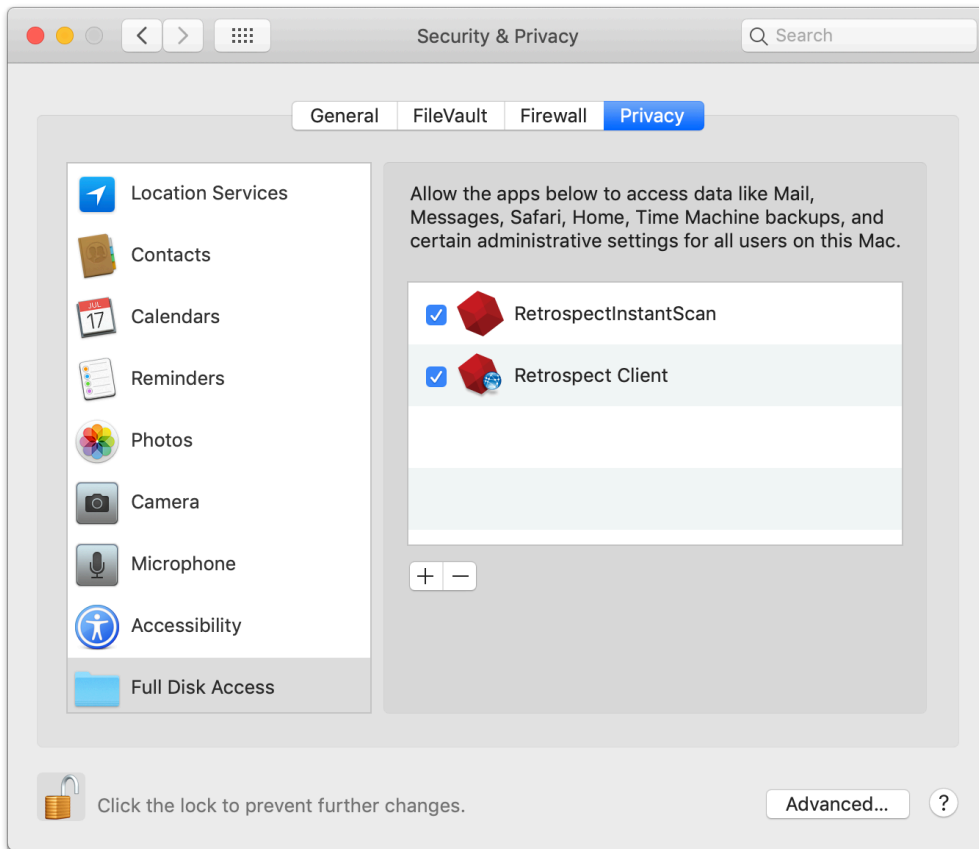
Click on the lock to authenticate and allow changes.

Now you need to find the Retrospect applications to drag into this list. Go to "Finder". Select "Go" from the menu bar and then "Go to Folder...". Enter:

```
/Library/PreferencePanels (Retrospect Client)
```

```
/Library/Application Support/Retrospect (RetrospectInstantScan)
```

Scroll down "Retrospect Client" (from the first folder) and "RetrospectInstantScan" (from the second folder) and drag them into the "Full Disk Access" list. Close "System Preferences".



Security and Encryption

Retrospect Backup protects your data in-transit and at-rest with industry-standard encryption algorithms. Let's walk through the different ways that your data is encrypted:

At-Rest Encryption

Retrospect Backup supports AES-256 encryption for all backup sets stored on any media, encoded on host, so your backups are encrypted before they touch the destination. That means cloud storage providers will never be able to access your data, but it also means no one can recover your data if you lose the encryption key.

In-Transit Encryption

Retrospect Backup supports a number of different network connections:

Clients: The agent-based connection is encrypted with AES-256 between the Retrospect Backup instance and the Retrospect Client agent for Windows, Mac, and Linux. For client-based history, on-demand backup, and on-demand and restore, the network connection is encrypted with AES-128.

Console: If you use the Retrospect Console for Mac on a different computer than the Retrospect Backup instance, the network connection is encrypted with AES-128.

Cloud Storage: The network connection is encrypted with HTTPS using TLS between the Retrospect Backup instance and the cloud storage provider. It supports up to TLS 1.2.

Retrospect Management Console: The network connection is encrypted with HTTPS using TLS between the Retrospect Backup instance and console.retrospect.com. It supports up to TLS 1.2.

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*.

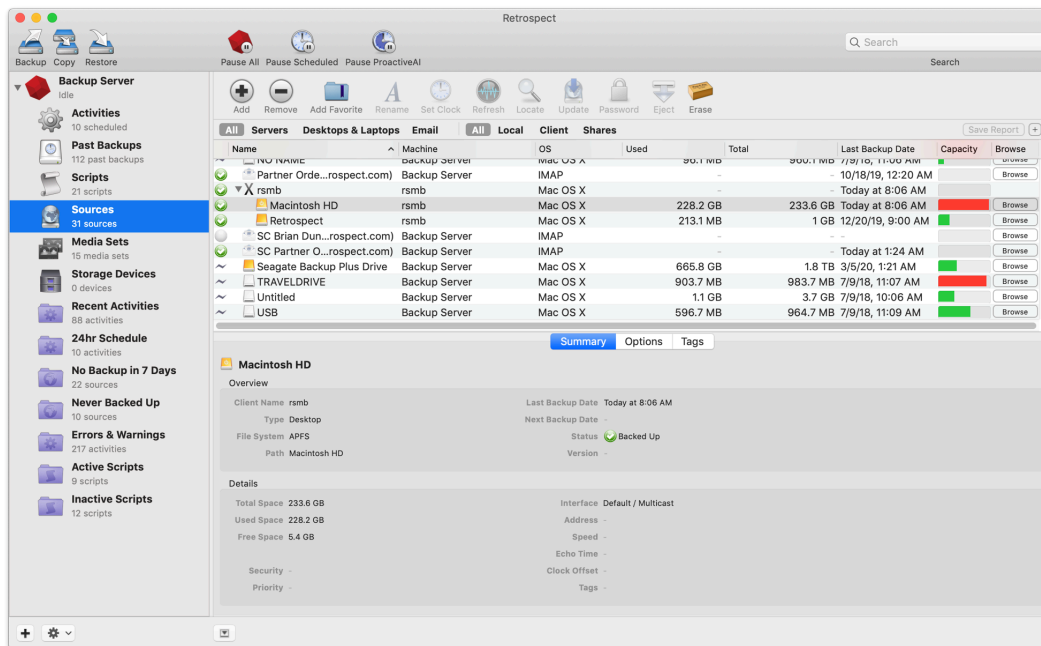
All of the backup, copy, and restore operations in Retrospect require a source and a destination. For a backup, the source is generally a hard drive or a folder on a hard drive (Retrospect calls these sources and Favorite Folders, respectively). The destination is generally a Media Set stored on backup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



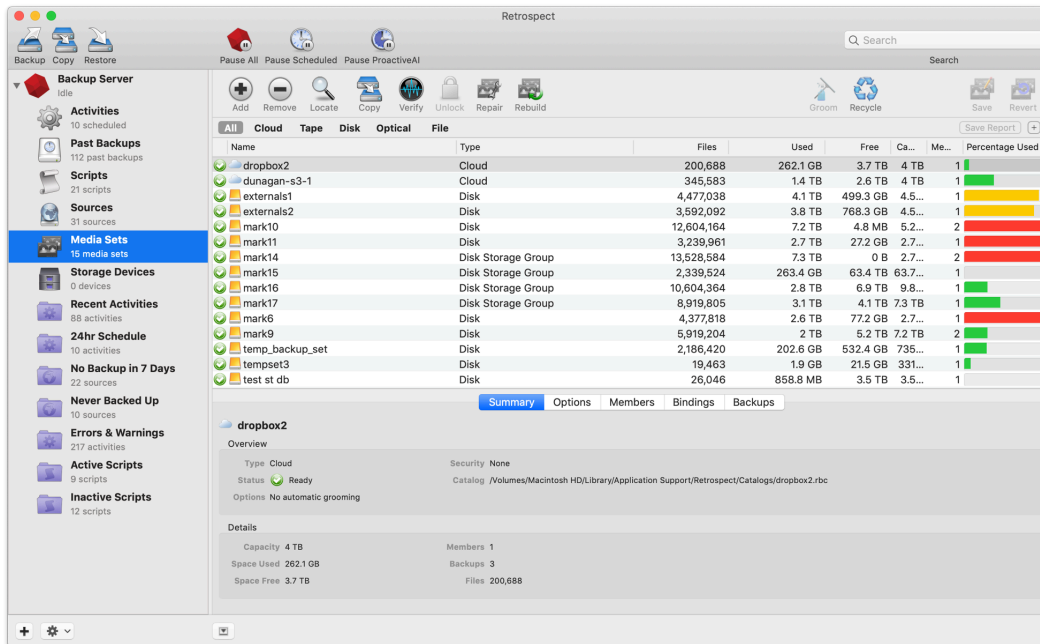
Above the Sources list, the toolbar allows you to add or remove sources, add Favorite Folders, and otherwise work with items in the Sources list. Below the list, a tabbed area allows you to see important details on a source that you have selected in the list.

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.

Storage Groups

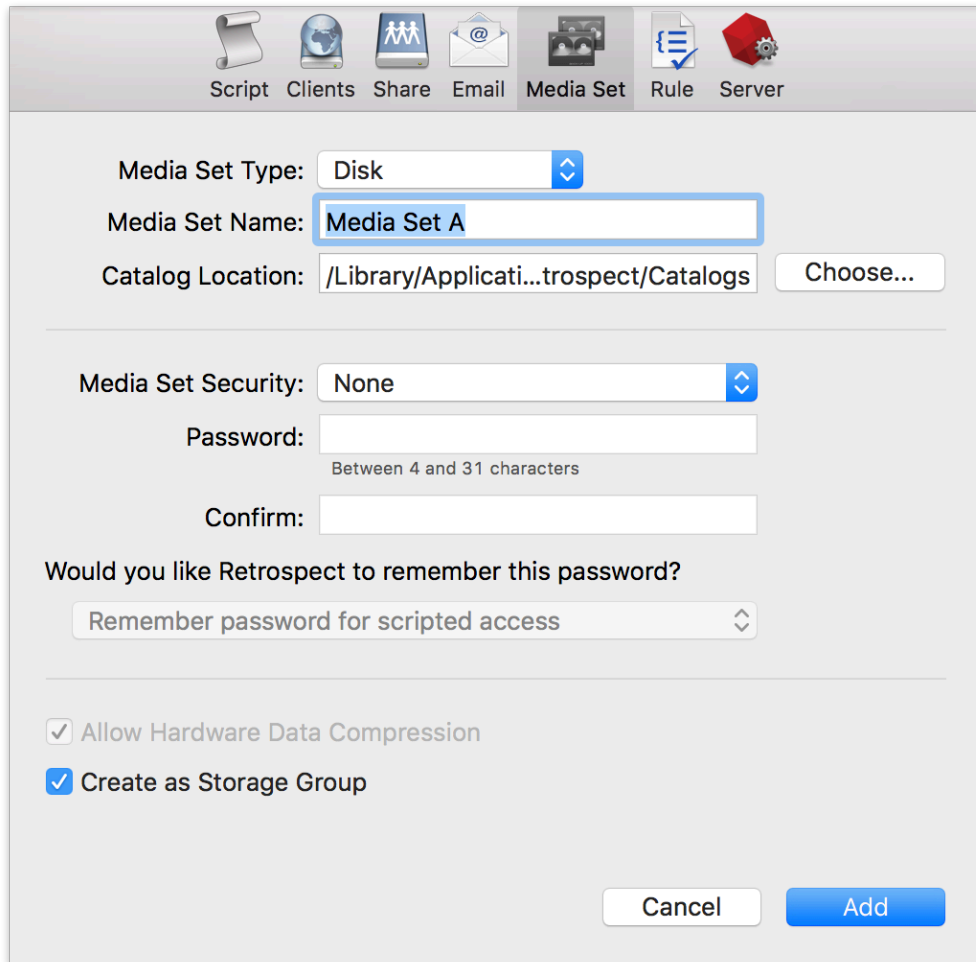
Storage Groups protect your entire backup environment up to 16x faster with a single, centralized disk or cloud destination that Retrospect can use simultaneously. With Storage Groups, you can run parallel backups to the same disk destination with a single ProactiveAI script. Scheduled scripts support Storage Groups as destinations, but the backups run on a single execution and not in parallel.

Storage Groups support the same workflows that you are accustomed to for backup, restore, transfer, grooming, and catalog rebuild, while providing far better performance and simplicity. You can treat the Storage Group like a Backup Set that allows simultaneous writes to it.

Creation

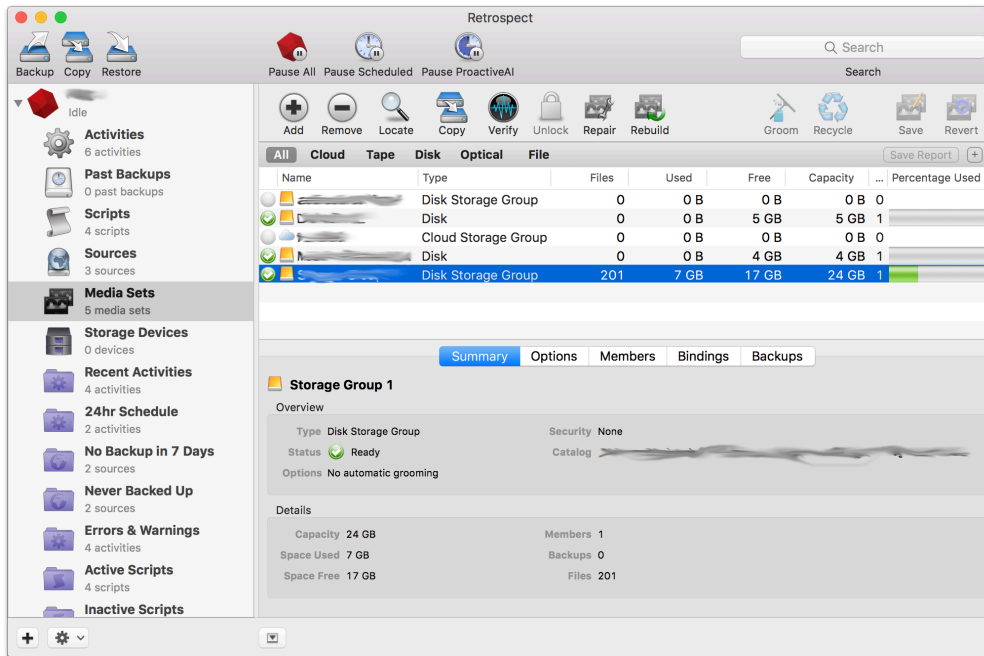
When creating a backup set, you will see "Create as Storage Group" as an option for disk sets and cloud sets. You can create one and use it as a destination for ProactiveAI scripts. If you select multiple sources for the script, they will run backups in parallel to the storage group.

The standard Retrospect Backup workflows for backups, restores, transfers, grooming, and rebuilds are the same for Storage Groups.



View

Storage Groups appear under the Backup Sets dialog on Windows and in the Media Sets tab on Mac.

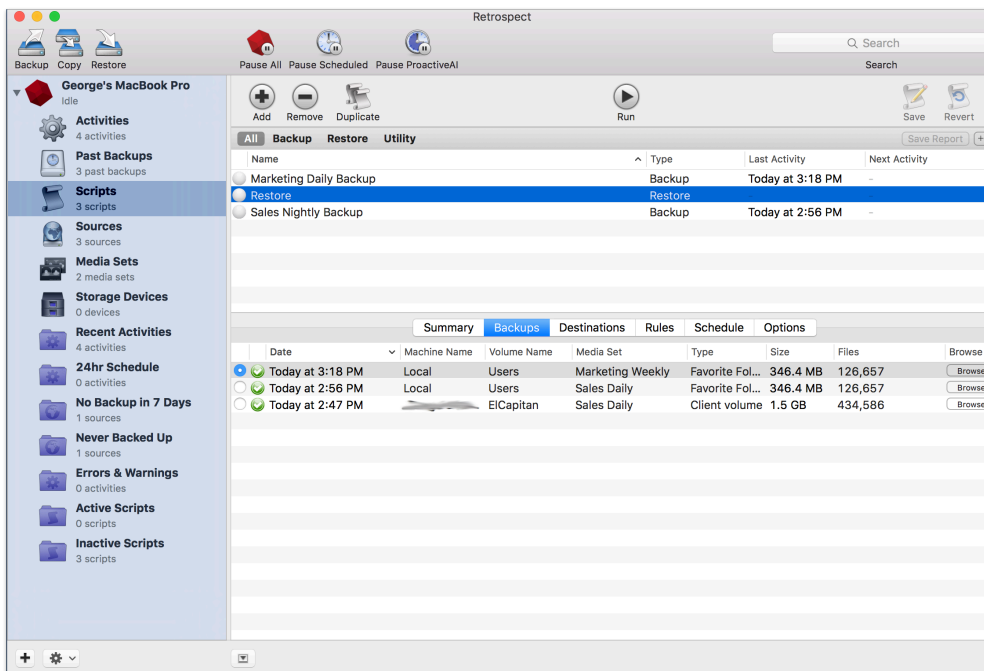


Backup

For backup, a Storage Group can be treated like a backup set. Select the Storage Group as the destination in your ProactiveAI script.

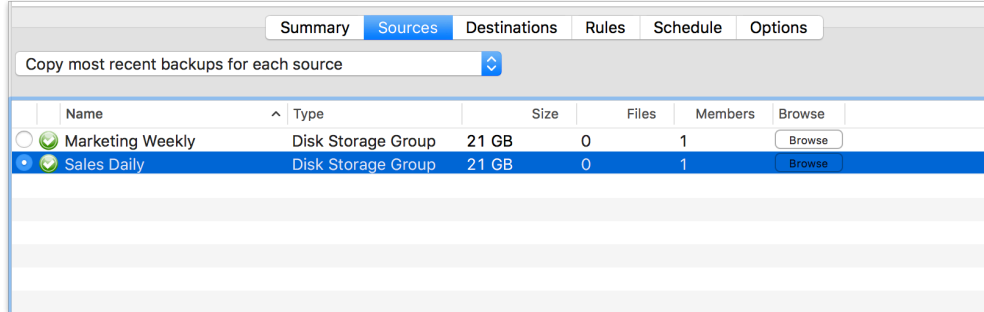
Restore

For restore in Retrospect for Mac, a Storage Group can be treated like a media set.

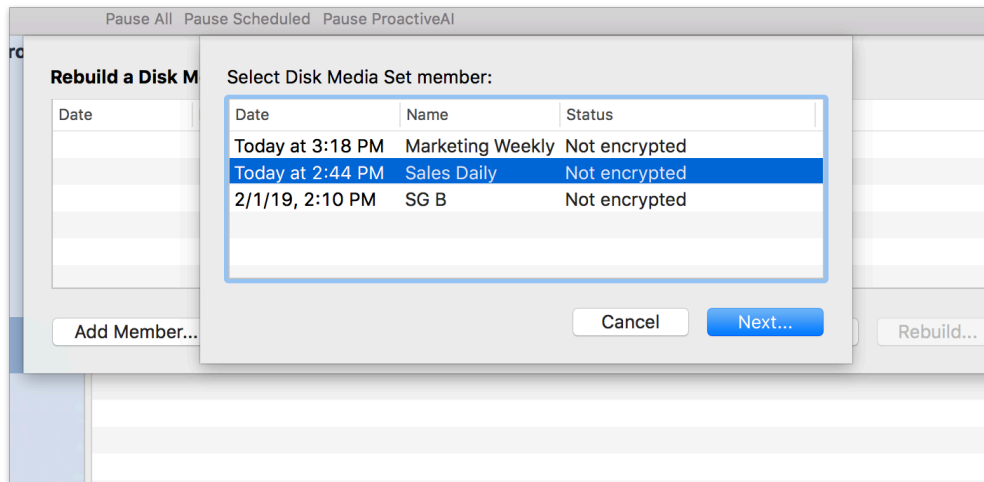


Transfer

For transfer in Retrospect for Mac, a Storage Group can be treated like a media set.



Rebuild



Mac

Verify

For verify in Retrospect for Mac, a Storage Group can be treated like a media set. The user interface is the same.

Under the Hood

Under the hood, a Storage Group is a container for per-volume backup sets. This architecture is why Retrospect allows you to keep the same workflows that you are accustomed to for backup, restore, transfer, grooming, and catalog rebuild, while providing far better performance and simplicity. You can treat the Storage Group like a Backup Set that allows simultaneous writes to it.

Data Deduplication

The architecture for Storage Groups allows simultaneous operations to the same destination because

each volume is a different backup set under the hood. However, this workflow also prevents data deduplication across volumes.

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.

ProactiveAI Backup

ProactiveAI is the next generation of Retrospect's Proactive scheduling engine. With ProactiveAI, backup scripts will optimize the backup window for the entire environment to ensure every source is protected as often as possible.

Algorithm

ProactiveAI walks through the following algorithm to prioritize what to back up next:

Verify backup window: ProactiveAI only runs when it's allowed to. To restrict the backup window, go to the script's schedule.

Verify an execution unit is available: ProactiveAI only runs when an execution unit is available.

Ignore last backup time: Retrospect can back up every hour, every day, every Sunday, or any other schedule. As soon as ProactiveAI sees a new backup window (i.e. a new day), it will attempt to back up the sources. In contrast, previous versions of Retrospect would respect the time at which the last backup occurred. See "[Backup Window](#)" for more details.

Ignore unavailable sources: If a source is unavailable, Retrospect will not attempt to reach it again until every potentially available source has been contacted. This list includes Wake-on-LAN sources. See "[Wake-on-LAN](#)" for more details.

Prioritize by next day: For all available or potentially available sources, Retrospect divides them into buckets for what day they are scheduled to be backed up next.

Using a future date might seem strange, but it can be in the past as well. This sorting algorithm ensure Retrospect prioritizes initial backups and then overdue backups. Think of it as last backup day combined with the script's schedule. As an example, Script A with weekly backups and Script B with daily backups would calculate the next backup date differently.

Prioritize by last time checked: When Retrospect reaches out to a source, it marks that time in its

configuration. ProactiveAI uses this time to ensure it doesn't re-check sources that it already checked but couldn't find, so that the script can get through the entire list of sources before circling back.

Prioritize by the last backup's duration: Now that Retrospect is down to sources within the same day of priority, ProactiveAI sorts them based on the last backup's duration. Sources with faster previous backups will be backed up sooner than sources with slower previous backups.

As a real-life example, incremental backups of email services are fast, so those would be prioritized over a longer server backup. Because of this sorting, Retrospect will protect more sources throughout the day, but if a long server backup does not happen on a given day, its backup will be automatically given higher priority because its next backup was the day before.

Our Engineering team experimented with more data points, but the resulting sort order was too prone to hysteresis. In other words, if Retrospect includes more past data, including backup durations that were anomalies, the future prioritization continued to be affected for longer than we thought was useful.

Default to prior order: If there is no duration, ProactiveAI uses the prior order. For instance, if it's the first set of backups, they will occur as sources are available.

Connect to the next source: Retrospect will attempt to back up the selected source. If it's not available, Retrospect marks that time and moves on. If Retrospect times out and the client and script have Wake-on-LAN (WAL) set, Retrospect sends a WAL packet, waits three minutes, then tries to connect again. If that connection times out, Retrospect marks the sources as unavailable and moves on.

Record next backup date: After a successful backup, Retrospect marks the next backup date for the source and moves on. As discussed earlier, this future date varies based on the script's schedule.

Backup Window

Retrospect begins a backup as soon as a source becomes available. If Alice's laptop was backed up at 2:30pm yesterday, ProactiveAI will attempt to back up her laptop as soon as it comes online today, even if that's before 2:30pm.

This change corrects a long-standing issue with drift, and for existing customers, this new schedule represents a significant change from previous versions. In the past, Proactive used the "Last Backup Time" to determine when to next back up a source. If Alice's laptop was backed up at 2:30pm yesterday, an older version of Proactive would wait until 2:30pm today to attempt the next backup, regardless of whether it was idle and Alice's laptop was available.

Alice might have only opened her laptop at 2:30pm yesterday, but ever other day, she is online at 9am. Without this change, every future backup would have been at 2:30pm or later until she missed a day. Instead, her laptop is protected as soon as it's available for each backup window. For fine-grain scheduling, customers can use multiple ProactiveAI scripts with different schedules.

Wake-on-LAN

ProactiveAI is better optimized for handling [Wake-on-LAN \(WAL\)](#) sources. If the source has WAL enabled or the script has WAL enabled, ProactiveAI will include WAL packets in its operation. For each WAL source, Retrospect attempts a connection. If that times out after one minute, it sends a WAL packet, waits three minutes, and then attempts another connection. If that times out after one minute, ProactiveAI marks the source as unavailable, moves on, and will not attempt another connection until it has contacted each subsequent source.

In previous versions, Proactive would continue to attempt to wake up unresponsive or absent machines. For environments that had many laptops or otherwise unavailable machines, this workflow meant that Retrospect would spend a disproportionate amount of time looking for machines instead of backing up available machines.

Troubleshooting

ProactiveAI includes detailed logging to understand the choices it's making to optimize the backup window:

Engine Log Level 4: What ProactiveAI is doing

Engine Log Level 5: What ProactiveAI is considering

See [Advanced Logging Options](#) for details about enabling logging.

Hardware

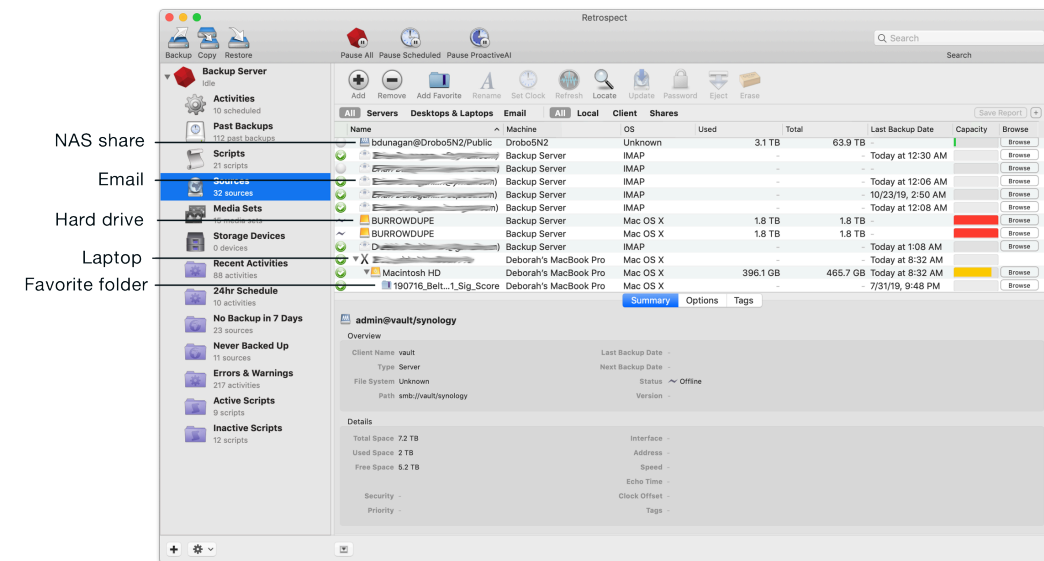
This chapter explains how Retrospect works with your different backup devices, and explains how you can see and control your hardware from within Retrospect.

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.

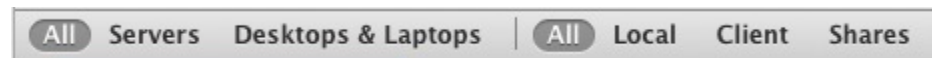
Password changes the login for the selected network share or Retrospect client computer.

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).

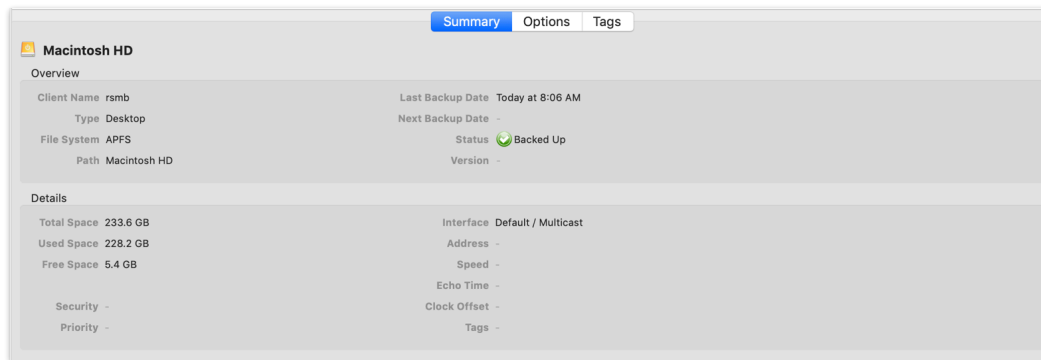
The second group allows you to filter the items in the Sources list by type. Clicking the Local button shows you Sources connected to the Retrospect server computer. Clicking the Client button shows you only the Retrospect client computers. Clicking the Shares button shows you only network shares.

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 ProactiveAI 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 ProactiveAI 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.

Searching for sources by tag

Keyword tags are even more powerful in Retrospect with the addition of a Tags criteria in the Sources filter. Let's say all the portable computers in your organization have been given a "laptop" tag. The example below explains how to find them.

How to view sources with the tag “laptop”:

Click **Sources** in the sidebar.

Click the plus (+) button next to the Save Report button to display the filter toolbar.

Click the left-most drop-down list and select **Tags**.

Select **Contains** from the next dropdown.

Type *laptop* into the text-entry field, and press the **Return** key.

All sources with the “laptop” tag are displayed.

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).

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.

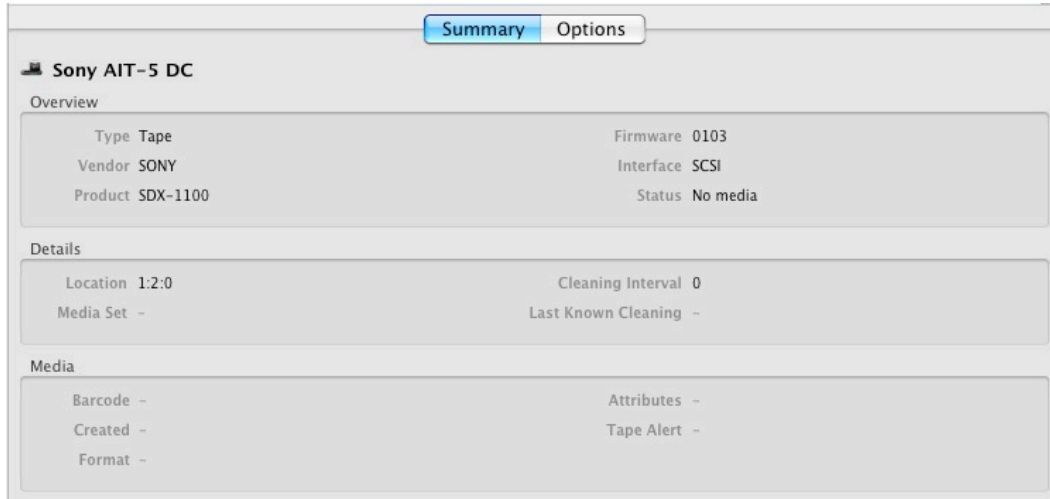
Status shows you the condition of the storage device, as reported by the device. For example, most tape drives will report Ready when there is a tape in the drive that can be written. In the screenshot below, because the device is a tape library, the Device Status for the first drive is 6: Ready, indicating 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

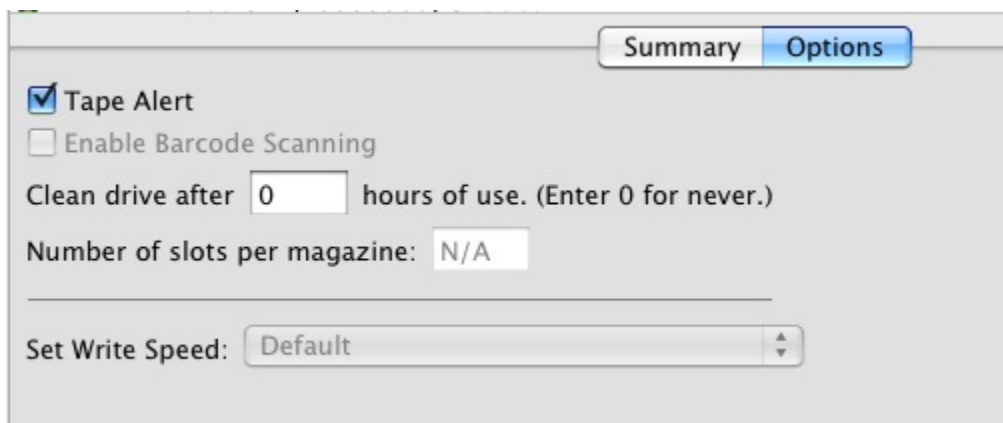
Below the Storage Devices list, the Detail area shows additional information about whichever device is selected in the list. There are two tabs in the Detail area: Summary and Options.

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 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.*

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:

Load the cleaning tape into an empty slot in the library.

Click Storage Devices in the sidebar.

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

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

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

To clean a tape drive manually:

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.

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:

Click Storage Devices in the sidebar.

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:

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.

Click to select the tape Media Set to which you want to add members.

In the detail area below the Media Sets list, click the Members tab.

Click the + (plus) button below the list.

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

Click Add.

Click Add.

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.

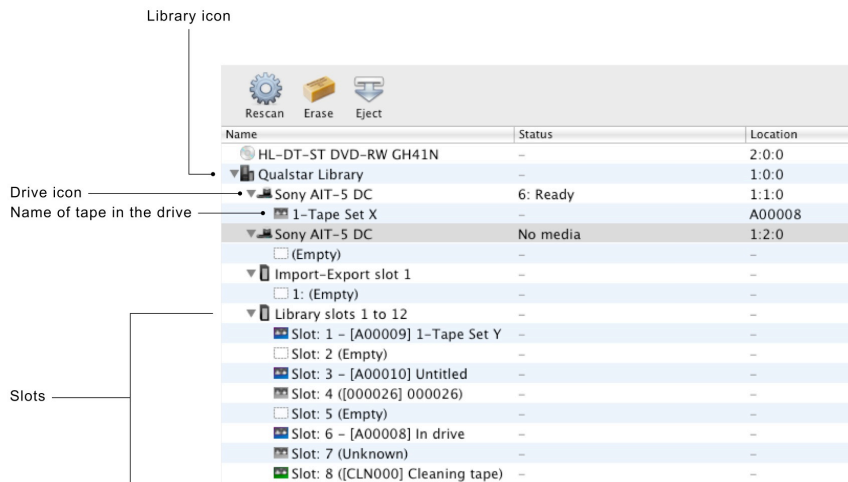
If your library does not support barcode reading, Retrospect must scan the library to get the name of each tape. The library inserts each tape in the tape drive, and Retrospect then keeps track of the tapes' names and locations.

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.

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.

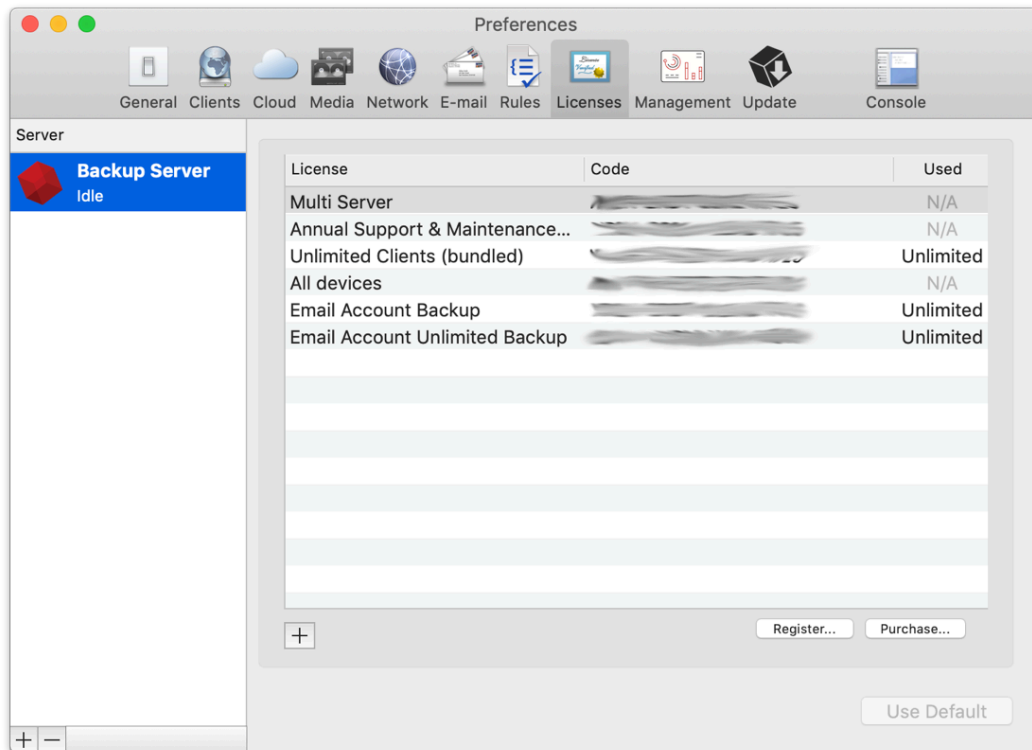
To back up clients, first install the Retrospect Client software on each of the client computers. Then use the Retrospect console application to add those clients as sources for use by the Retrospect server. After configuring the clients, you can create and schedule scripts using client volumes as sources,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

Launch the Retrospect application and choose Retrospect > 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.

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.)

From the Retrospect Installer disk image or CD, open the Client Installers folder, then copy the Mac Client Installer folder onto your hard drive.

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.

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.

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:

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.

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

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.

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.

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.

(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.

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:

In the sidebar, click on Sources.

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.

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:

In the sidebar, click on Sources.

In the Sources list, click to select the Retrospect client machine you wish to locate.

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:

In the sidebar, click on Sources.

Click the Add button in the toolbar. The Add Source dialog appears.

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.

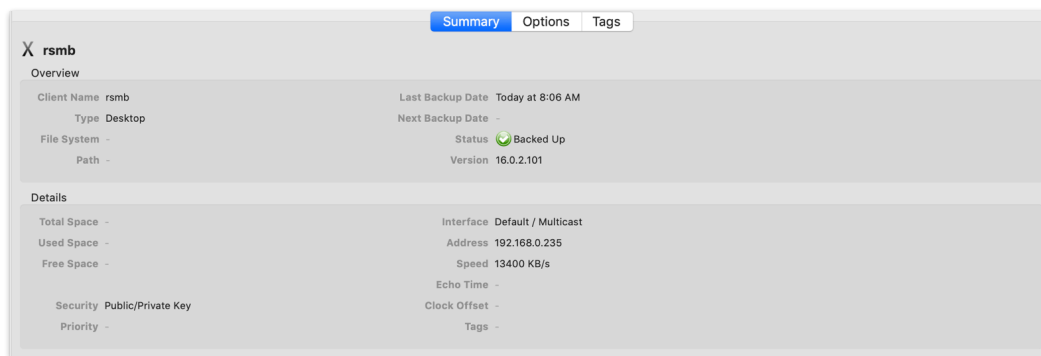
In the Sources list, select the client and choose Remove from the toolbar.

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:

In the sidebar, click on Sources.

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.

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](#).

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.

NOTE: You can find the RCU file on the Retrospect website under Downloads for a respective platform's client. You can also export it from Preferences > Console > Export Client Installer.

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 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

Locate your Retrospect disk image or CD and navigate to
`/Client Installers/Mac Client/.`

Copy the Mac Client Uninstaller to the Macintosh on which you want to uninstall the Retrospect Client software.

Open the Mac Client Uninstaller and follow the on-screen instructions to uninstall the Retrospect Client software.

Windows

From the Start menu, choose Settings > Control Panel (Windows XP) or Control Panel (Windows Vista and Windows 7).

Double-click Add/Remove Programs (Windows XP) or Programs and Features (Windows Vista and Windows 7).

In the window that appears, select the Retrospect Client software and click Change/Remove (Windows 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 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 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:

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.

Click the Add button in the List View toolbar. The Add Source dialog appears.

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`.

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 reenter the information.

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.

Adding network shares

Network shares can be backed up or used as a backup location. Retrospect supports AFP, SMB, and WebDAV shares. Identifying shares and adding them to your projects is now easier than ever.

To add a share as a source:

Click **Sources > Add > Share**. Enter the share address and any required log-in information.

To add a share as a backup location:

Click **Media Sets > Add > Share**. Enter the share address and any required log-in information.

New Retrospect Client software

Retrospect Client software allows individual users to control aspects of the backup and restore operations performed on their computers. The client software has been redesigned for Windows and Mac OS. The changes include:

An updated user interface with Windows taskbar and Mac menu bar integration

User-initiated backups and restores

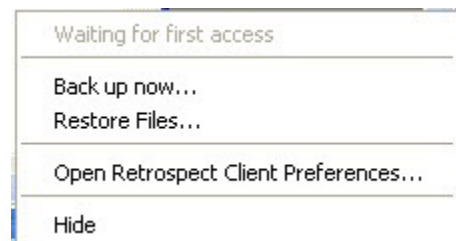
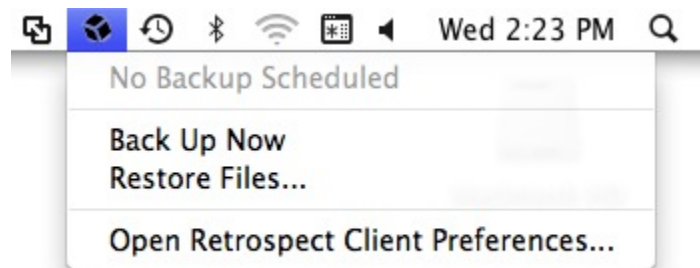
Better-organized preference panels with enhanced options

Link encryption employs strong AES-256 encryption

Note: The Retrospect system administrator has the ability to restrict access to some of these features. For more information, see [Locking client features and preferences](#).

User-initiated backups and restores

Users now have the ability to restore files and request backups directly from their desktop. When the Retrospect Client software is installed, a Retrospect icon is added to the Windows taskbar and Mac OS menu bar. Click the icon to open a menu you can use to initiate a backup or restore operation.



User-initiated backups

This backup method is best if you need to quickly protect a specific file or folder. It is not meant to be a substitute for regular backups and cannot be used to perform a full system backup of your computer.

To perform a user-initiated backup:

Click the Retrospect icon in the Windows taskbar or Mac OS menu bar.

Select **Back Up Now**.

Use the Backup Files and Folders dialog to select the items to back up.

Click **Back Up**.

Notes about user-initiated backups:

The Back Up Now and Restore Files menu items are inactive until the client computer has been logged into a Retrospect server where these options are activated.

Mac: By default, backed up files and folders are stored in a Media Set chosen by the system administrator in the Retrospect Client preferences. The Media Set is selected using the **Back up on demand to** popup list.

Windows: By default, backed up files and folders are stored in a Backup Set chosen by the system administrator in the Retrospect Client preferences. The Backup Set is selected using the **Back up on demand to** popup list.

User-initiated restores

Restores can be initiated from the client computer's taskbar or menu bar or by clicking the **Restore** button on the **Retrospect** Client preference pane's **History** tab.

To perform a user-initiated restore:

Click the Retrospect icon on the client computer's taskbar or menu bar.

Select **Restore Files** .

In the Restore Files and Folders window, select a backup from the menu that contains the files you would like to restore.

Select the files to restore.

Click **Restore** .

To choose a different location, click **Browse** . To continue, click **Restore** .

Improved client preferences

To open the Retrospect Client preference pane on Mac:

Click on the Retrospect menu icon on the menu bar. Select **Open Retrospect Client Preferences**.

Click **System Preferences** in the Dock. Click the Retrospect Client icon.

From the Apple menu, choose **System Preferences**. Click the Retrospect Client icon.

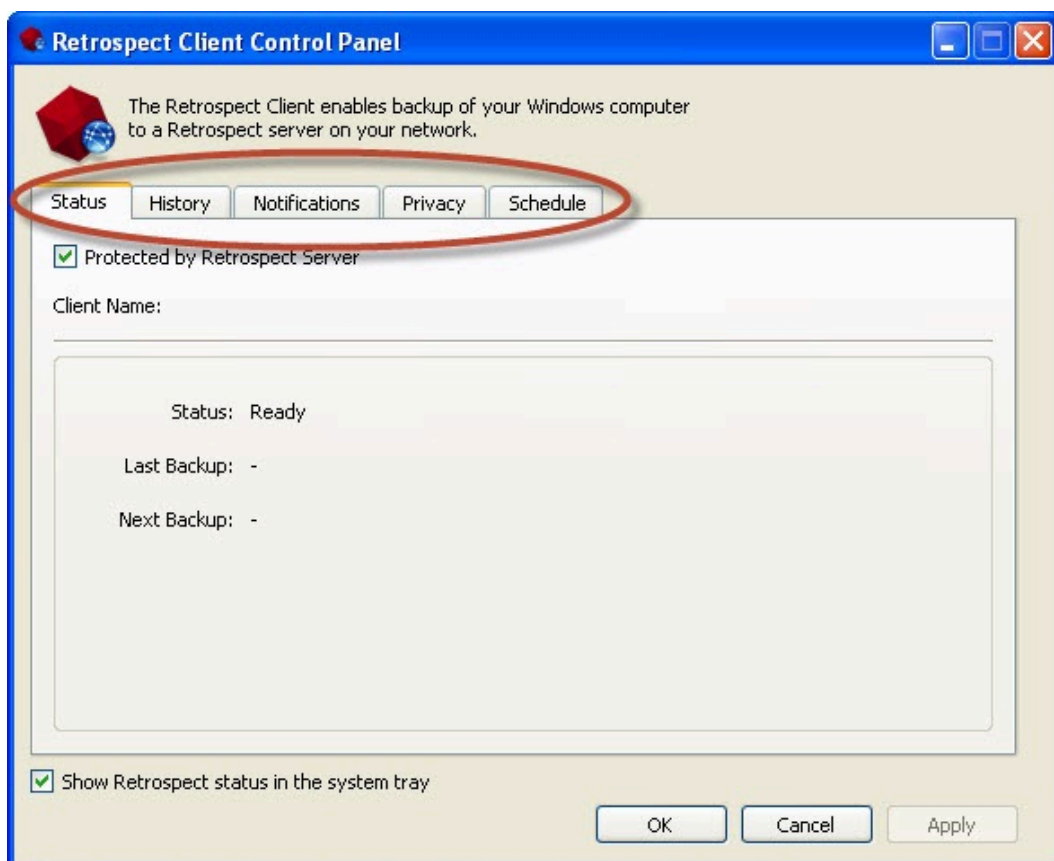
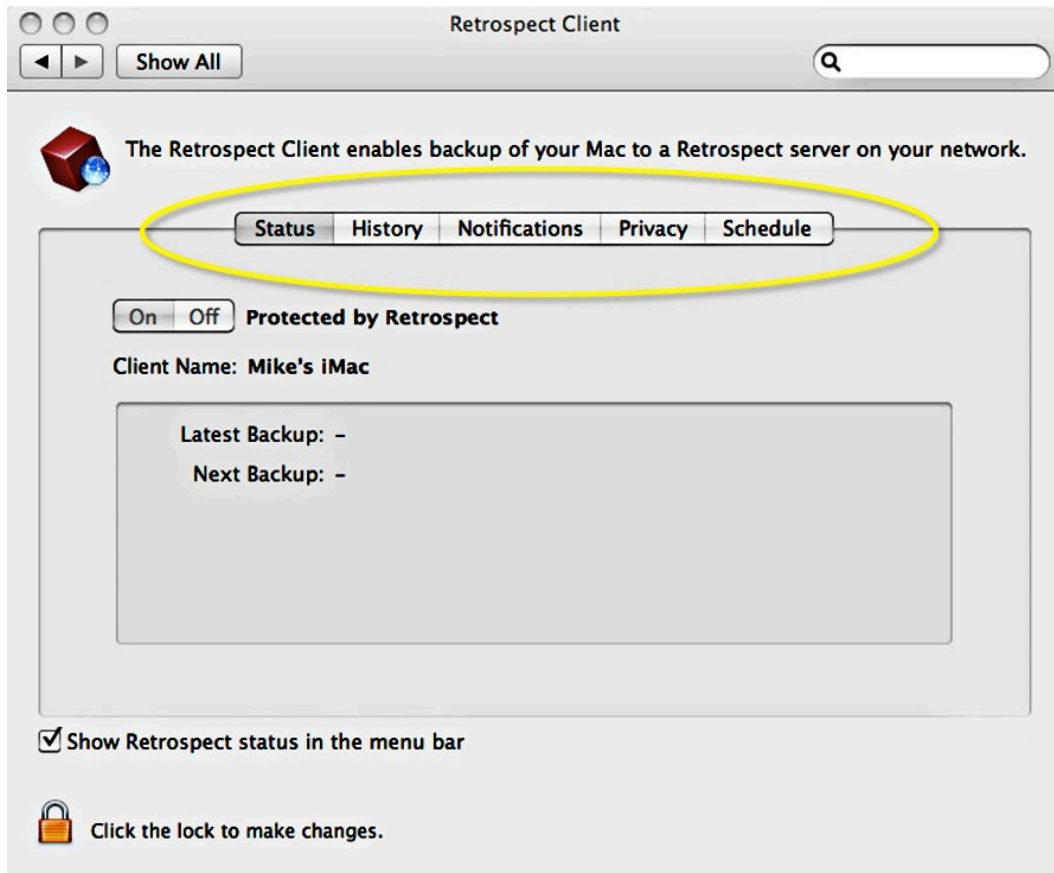
To open the Retrospect Client control panel on Windows:

Click **Start > Programs (or All Programs) > Retrospect > Retrospect Client**.

From the Windows taskbar, click the Retrospect Client icon and select **Open Retrospect Client Preferences**.

Setting client preferences

Preferences are grouped into the following categories: Status, History, Notifications, Privacy, and Schedule. Click one of the category buttons to access the settings.



Status preferences

Protected by Retrospect Server : ** Use this option to disable access to the client by the backup computer.

Client Name : The client name and the client IP address being used by Retrospect are displayed here.

Status area : Information about your latest and next backups are displayed. If a backup is running, a progress bar is shown.

History preferences

History area : Your disk-based backups are listed here. In each row you will find information about the backup and a **Restore** button. A green icon indicates the backup completed successfully. A yellow icon indicates there was a problem with one or more files in the backup. A red icon indicates the backup failed. To start a restore operation using one of these backups, click the corresponding **Restore** button.

Notifications preferences

Notify after backup : Displays a message after the completion of a backup or other operation.

Notify if no backup in *N* days : Displays a message if the client has not been backed up within the number of days specified in the entry box.

Report SMART errors : Requests an immediate backup from ProactiveAI Backup (if applicable) when Retrospect learns of errors on the client's SMART hard drive volumes. This setting is off by default.

Privacy preferences

Privacy area : This area displays any files or folders designated as Private. Private files are not visible to the Retrospect server and are not backed up. Drag volumes, files or folders to this panel to designate them as Private.

Add/Remove buttons : To add files or folders to your Privacy list, click the **Add** button and navigate to the files or folders you wish to add. To remove an item from your list, select it in the Exclude area, and click the **Remove** button.

Allow Retrospect to change files on my system (Required for restore): When this option is unchecked, the client can be backed up, but files on the client cannot be restored, modified, or deleted by the backup computer. This setting is on by default.

Schedule preferences

Delay ProactiveAI Backups until after [date & time] : 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 or click the arrows to make changes.)

Locking client features and preferences

The Retrospect system administrator has the ability to prevent users from changing certain client settings. For instance, you may not want users to prevent their computers from being backed up.

The most efficient workflow for a system administrator is to establish a set of standard lockout preferences, and then make any desired customizations on a client-by-client basis. The steps below explain how to do this.

To set the default lockout preferences:

The lockout controls are in the Retrospect console. **Mac:** Choose **Retrospect > Preferences > Clients** tab. **Windows:** Choose **Configure > Preferences > Allow Clients to** in the Retrospect console sidebar.

In the **Allow Clients to** section, modify one or more of the following preferences:

Turn off the Retrospect Client software : When checked, this preference allows users to hide their client from the Retrospect server. All communication between the server and the client will be cut. Any backups scheduled to run while the client is turned off will be skipped.

Stop running backups : When checked, this preference allows client users to stop operations that are in progress.

Exclude items from backups : When checked, this preference allows users to mark files, folders, and volumes as Private, making them invisible to Retrospect.

Set read access only : When checked, this preference allows clients to prevent Retrospect from writing to or deleting files on their computer.

Back up on demand to : When checked, this preference allows clients to initiate on-demand backups to the Disk Media Set selected in this popup menu. When checked, this preference allows clients to initiate on-demand backups to the selected Backup Set. Click **Select Backup Set...** to choose a Backup Set.

Restore on demand : When checked, this preference allows clients to initiate on-demand restores from available Backup Sets. When checked, this preference allows clients to initiate on-demand restores from available Disk Media Sets.

To customize these default preferences for an individual client:

Mac: Select **Sources** in the Retrospect console sidebar. **Windows:** Select **Configure > Clients** in the Retrospect sidebar.

Select a client from the list.

Mac: Click the **Details > Options** tab. **Windows:** Click **Properties**.

Modify the preference settings as desired for this client.

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:

In the Retrospect console, click on Sources in the sidebar.

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

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 example, 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:

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.

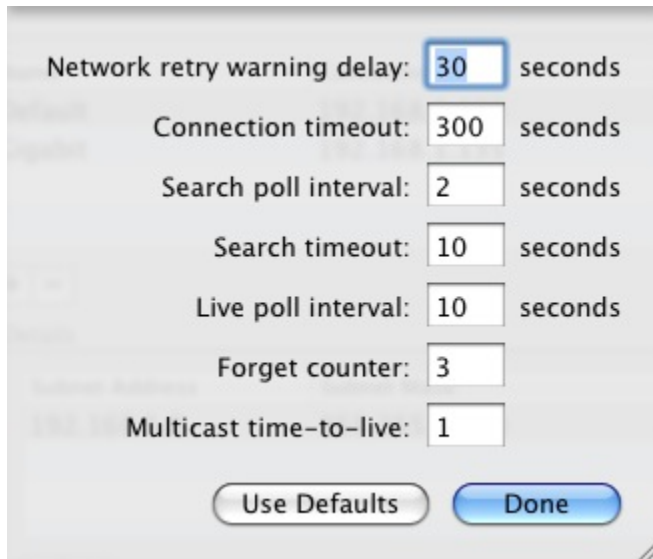
To add another network interface, click the Plus (+) button below the connection list. In the resulting dialog, choose from the Connection pop-up menu the IP address of the network interface you want to use, then enter a name for the connection and click Add.

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 ProactiveAI 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.)

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 ProactiveAI 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, 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:

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.

In the List View toolbar, click Add. The Media Set creation dialog appears.

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.

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

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.

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.

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.

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):

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

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.

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:

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.

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.

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.

Click Continue. The Select Media Sets pane appears, with a list of Media Sets.

If you previously created a Media Set as the destination for this backup, 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.

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.

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.

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.

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

(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.

(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.

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:

In the Retrospect console's Sidebar, click Scripts. A list of previously created scripts (if any) appears on the right side of the window.

In the List View Toolbar, click the Add button. The Script dialog appears.

In the Script Name field, enter a name for your new script.

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.

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.

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.

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.

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.

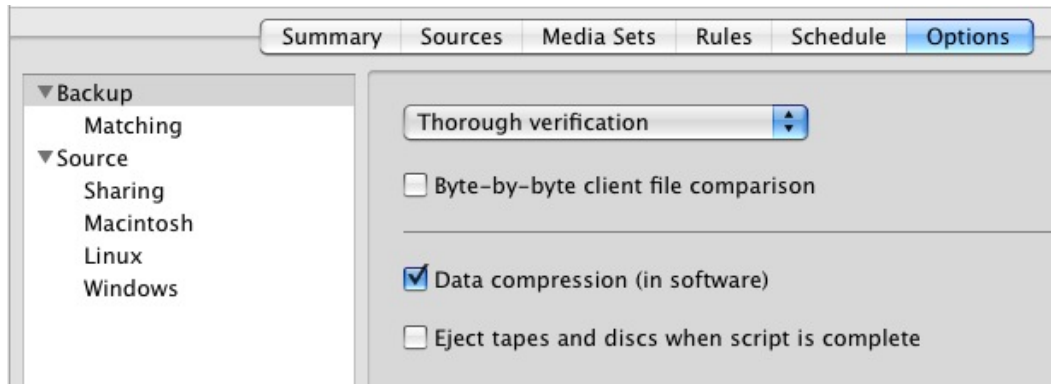
In the schedule interface, the Destination pop-up menu lists the Media Sets that you previously selected. If more than one Media Set is associated with this Script, choose the one you want for this schedule from the pop-up menu. Next, choose the Media action that you want (the choices are No media action, 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.

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

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 ProactiveAI 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 MacOS 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

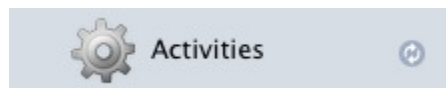
One of the things you will probably want to do often is monitor Retrospect's progress during an operation, especially if it is the first time you are running the script that controls the operation. To do this, follow these steps:

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

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.

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 ProactiveAI 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.

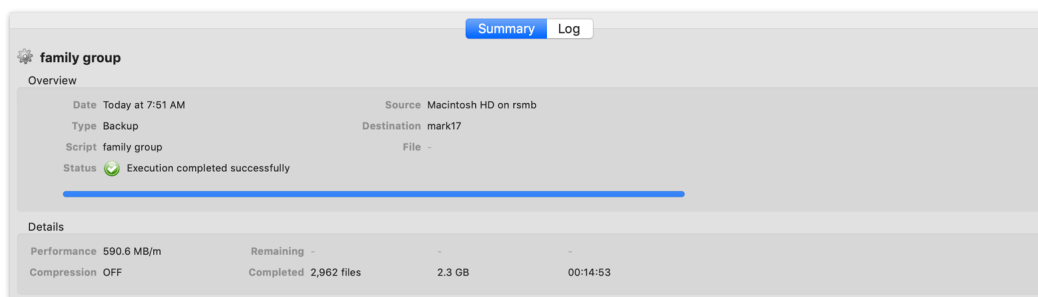
Customizing the Activity List

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.

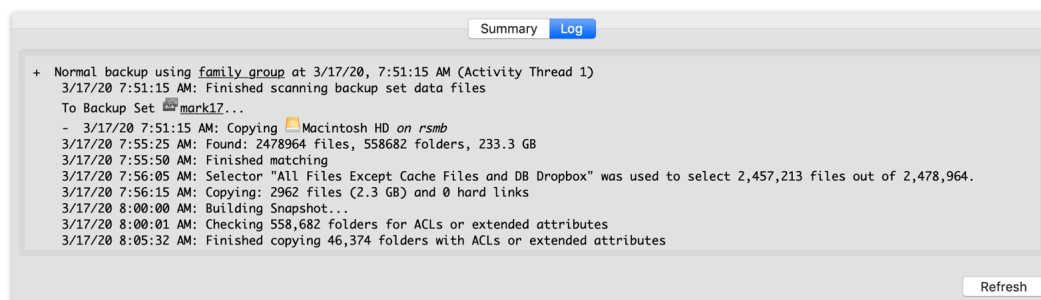


The screenshot shows the 'Summary' tab for a backup activity. The activity is named 'family group' and was performed 'Today at 7:51 AM'. The source is 'Macintosh HD on rsmb' and the destination is 'mark17'. The script used is 'family group' and the status is 'Execution completed successfully'. The details section shows a performance of 590.6 MB/m, 2,962 files completed, 2.3 GB of data, and a duration of 00:14:53.

Overview	
Date	Today at 7:51 AM
Type	Backup
Script	family group
Status	Execution completed successfully
Source	Macintosh HD on rsmb
Destination	mark17
File	-

Details			
Performance	590.6 MB/m	Remaining	-
Compression	OFF	Completed	2,962 files
			2.3 GB
			00:14:53

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

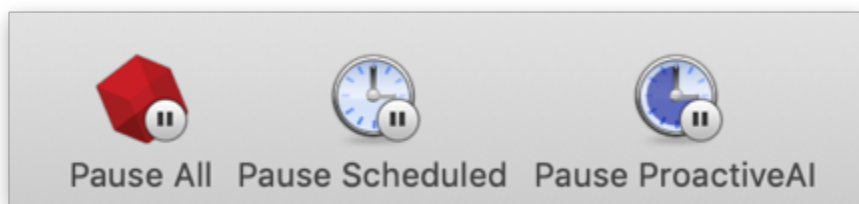


Note: For currently executing activities, click the refresh button to see the latest information about the activity.

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 ProactiveAI 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 ProactiveAI Backup scripts. When Retrospect Clients associated with ProactiveAI 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.

ProactiveAI Backup

ProactiveAI is the next generation of Retrospect's Proactive scheduling engine. With ProactiveAI, backup scripts will optimize the backup window for the entire environment to ensure every source is protected as often as possible.

Algorithm

ProactiveAI walks through the following algorithm to prioritize what to back up next:

Verify backup window: ProactiveAI only runs when it's allowed to. To restrict the backup window, go to the script's schedule.

Verify an execution unit is available: ProactiveAI only runs when an execution unit is available.

Ignore last backup time: Retrospect can back up every hour, every day, every Sunday, or any other schedule. As soon as ProactiveAI sees a new backup window (i.e. a new day), it will attempt to back up the sources. In contrast, previous versions of Retrospect would respect the time at which the last backup occurred. See "[Backup Window](#)" for more details.

Ignore unavailable sources: If a source is unavailable, Retrospect will not attempt to reach it again until every potentially available source has been contacted. This list includes Wake-on-LAN sources. See "[Wake-on-LAN](#)" for more details.

Prioritize by next day: For all available or potentially available sources, Retrospect divides them into buckets for what day they are scheduled to be backed up next.

Using a future date might seem strange, but it can be in the past as well. This sorting algorithm ensure Retrospect prioritizes initial backups and then overdue backups. Think of it as last backup day combined with the script's schedule. As an example, Script A with weekly backups and Script B with daily backups would calculate the next backup date differently.

Prioritize by last time checked: When Retrospect reaches out to a source, it marks that time in its configuration. ProactiveAI uses this time to ensure it doesn't re-check sources that it already checked but couldn't find, so that the script can get through the entire list of sources before circling back.

Prioritize by the last backup's duration: Now that Retrospect is down to sources within the same day of priority, ProactiveAI sorts them based on the last backup's duration. Sources with faster previous backups will be backed up sooner than sources with slower previous backups.

As a real-life example, incremental backups of email services are fast, so those would be prioritized over a longer server backup. Because of this sorting, Retrospect will protect more sources throughout the day, but if a long server backup does not happen on a given day, its backup will be automatically given higher priority because its next backup was the day before.

Our Engineering team experimented with more data points, but the resulting sort order was too

prone to hysteresis. In other words, if Retrospect includes more past data, including backup durations that were anomalies, the future prioritization continued to be affected for longer than we thought was useful.

Default to prior order: If there is no duration, ProactiveAI uses the prior order. For instance, if it's the first set of backups, they will occur as sources are available.

Connect to the next source: Retrospect will attempt to back up the selected source. If it's not available, Retrospect marks that time and moves on. If Retrospect times out and the client and script have Wake-on-LAN (WAL) set, Retrospect sends a WAL packet, waits three minutes, then tries to connect again. If that connection times out, Retrospect marks the sources as unavailable and moves on.

Record next backup date: After a successful backup, Retrospect marks the next backup date for the source and moves on. As discussed earlier, this future date varies based on the script's schedule.

Backup Window

Retrospect begins a backup as soon as a source becomes available. If Alice's laptop was backed up at 2:30pm yesterday, ProactiveAI will attempt to back up her laptop as soon as it comes online today, even if that's before 2:30pm.

This change corrects a long-standing issue with drift, and for existing customers, this new schedule represents a significant change from previous versions. In the past, Proactive used the "Last Backup Time" to determine when to next back up a source. If Alice's laptop was backed up at 2:30pm yesterday, an older version of Proactive would wait until 2:30pm today to attempt the next backup, regardless of whether it was idle and Alice's laptop was available.

Alice might have only opened her laptop at 2:30pm yesterday, but ever other day, she is online at 9am. Without this change, every future backup would have been at 2:30pm or later until she missed a day. Instead, her laptop is protected as soon as it's available for each backup window. For fine-grain scheduling, customers can use multiple ProactiveAI scripts with different schedules.

Wake-on-LAN

ProactiveAI is better optimized for handling [Wake-on-LAN \(WAL\)](#) sources. If the source has WAL enabled or the script has WAL enabled, ProactiveAI will include WAL packets in its operation. For each WAL source, Retrospect attempts a connection. If that times out after one minute, it sends a WAL packet, waits three minutes, and then attempts another connection. If that times out after one minute, ProactiveAI marks the source as unavailable, moves on, and will not attempt another connection until it has contacted each subsequent source.

In previous versions, Proactive would continue to attempt to wake up unresponsive or absent machines. For environments that had many laptops or otherwise unavailable machines, this workflow meant that Retrospect would spend a disproportionate amount of time looking for machines instead of backing up available machines.

Troubleshooting

ProactiveAI includes detailed logging to understand the choices it's making to optimize the backup window:

Engine Log Level 4: What ProactiveAI is doing

Engine Log Level 5: What ProactiveAI is considering

See [Advanced Logging Options](#) for details about enabling logging.

Creating a ProactiveAI Backup Script

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

To create a ProactiveAI Backup script, follow these steps:

In the Retrospect console's Sidebar, click Scripts. A list of previously created scripts (if any) appears on the right side of the window.

In the List View Toolbar, click the Add button. The Script dialog appears.

In the Script Name field, enter a name for your new script.

Make sure that the All or Backup category is selected, then click ProactiveAI 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.

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.

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 ProactiveAI Backup script to use any and all available backup media.

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

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.

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 ProactiveAI Backup script is set to run every day, all day.

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

Copying (Replication)

A Copy operation (also known as replication) 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:

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.

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.

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.

(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.

(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:

In the Retrospect console’s Sidebar, click Scripts. A list of previously created scripts (if any) appears on the right side of the window.

In the List View Toolbar, click the Add button. The Script dialog appears.

In the Script Name field, enter a name for your new Copy script.

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.

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.

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.

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.

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.

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.

Click the Options tab, then set the copy script options you desire. See “Copy Script Options” for more information.

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:

In the Retrospect console's Sidebar, click Scripts. A list of previously created scripts (if any) appears on the right side of the window.

In the List View Toolbar, click the Add button. The Script dialog appears.

In the Script Name field, enter a name for your new Archive script.

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.

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.

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.

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.

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.

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.

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

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.

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:

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

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

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.

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:

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.

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.

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

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.

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:

In the Retrospect console's Sidebar, click Scripts.

In the List View Toolbar, click the Add button. The Script dialog appears.

In the Script Name field, enter a name for your new Restore script.

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.

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.

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:

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

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.

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.

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 MacOS 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).

Restoring from Retrospect 6.x backups

Retrospect for Mac can restore from Backup Sets created by Retrospect 6.x for Mac (except those of type Internet). However, it is not possible to add more data to these Backup Sets using version 19; Retrospect for Mac treats version 6.x Backup Sets as read-only.

Before it's possible to search or restore from a 6.x Backup Set using Retrospect for Mac, a Retrospect for Mac Catalog must first be created. To create a version 19 Catalog from the 6.x media, go to the Media Sets view in Retrospect for Mac, click on the Rebuild button in the toolbar, add the Backup Set

members (like “1–Backup Set A” and “2–Backup Set A”) that contain the backup data, click Next, and then click Rebuild. You will need to tell Retrospect where to save the new Catalog. Retrospect will then scan over the backup media and generate a new Catalog. This will take some time. Once this process completes, you will be able to restore from that Backup Set.

To rebuild a Catalog from an Optical Disc Backup Set, it is first necessary to activate optical device support. The [instructions for activating optical support](#) can be found in the Retrospect Knowledgebase.

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:

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

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.

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.

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.

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.

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.

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.

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 backups 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.

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:

In the Retrospect console's Sidebar, click Scripts.

In the List View Toolbar, click the Add button. The Script dialog appears.

In the Script Name field, enter a name for your new Copy Media Set script.

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.

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

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.

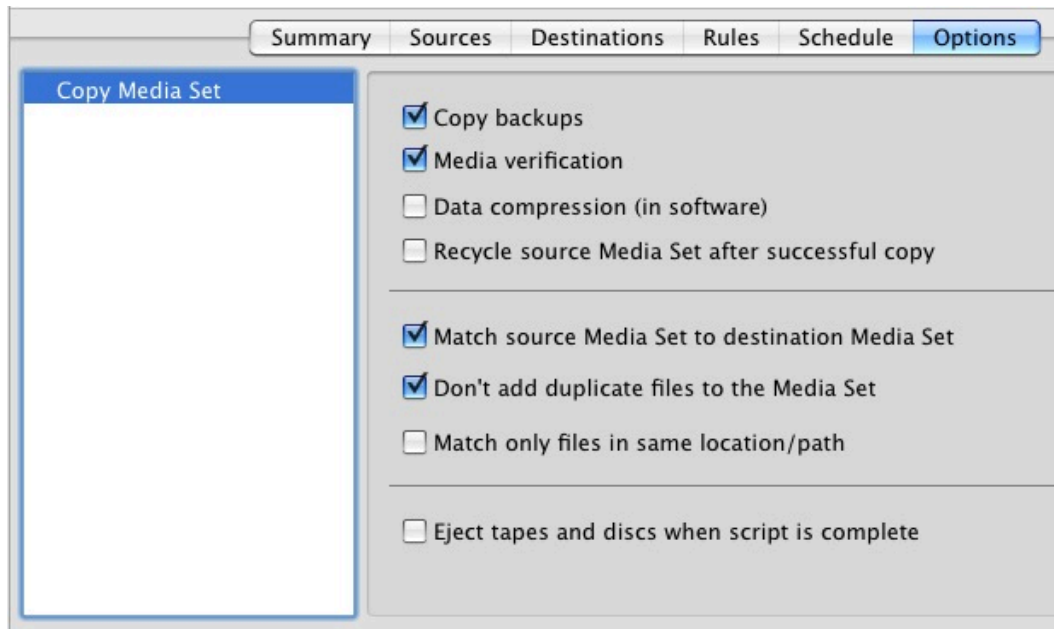
Click the Rules tab. Select the rule you want to apply to the backup.

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.

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:

In the Retrospect console's Sidebar, click Scripts.

In the List View Toolbar, click the Add button. The Script dialog appears.

In the Script Name field, enter a name for your new Copy Backup script.

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.

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

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.

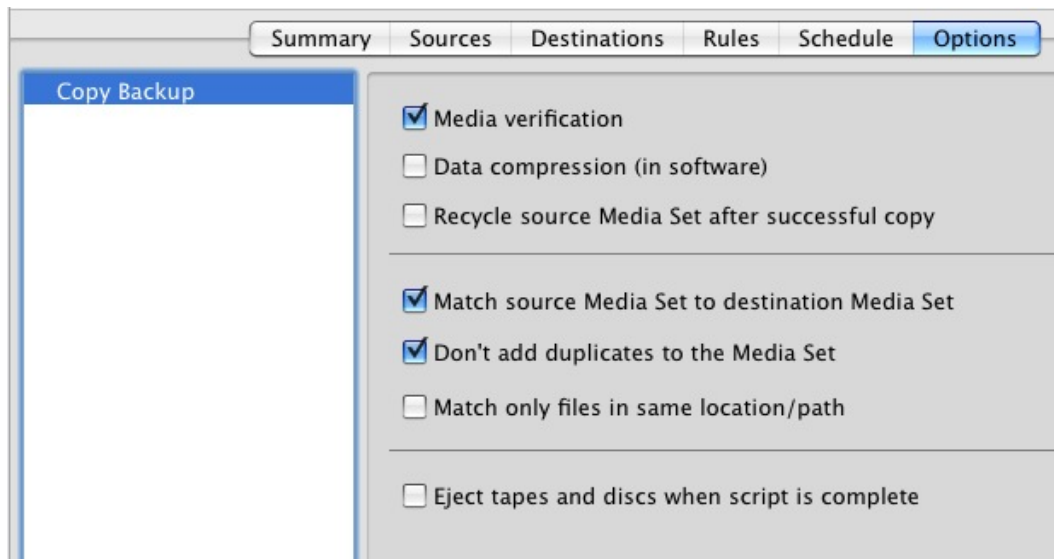
Click the Rules tab. Select the rule you want to apply to the backup.

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.

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:

In the Retrospect console’s Sidebar, click Scripts.

In the List View Toolbar, click the Add button. The Script dialog appears.

In the Script Name field, enter a name for your new Verifying script.

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.

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

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.

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:

In the Retrospect console's Sidebar, click Scripts.

In the List View Toolbar, click the Add button. The Script dialog appears.

In the Script Name field, enter a name for your new Groom script.

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.

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

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:

In the Retrospect console's Sidebar, click Scripts.

In the list of scripts, click to select the one you want to duplicate.

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.

Click on each of the tabs in the script's detail area and make the changes that you desire.

Filtering the contents of a past backup

While reviewing the contents of a past backup, you now have the option to view only the contents of the latest session. Double-click the name of a past backup to open the file list panel. To filter the list, select the **Show copied files only** check box.

Cloud Backup

Retrospect Backup allows you to protect your data in the cloud with seamless integration with the following unique features:

Multiple Providers: Retrospect supports more than twenty cloud storage providers, located around the world, for affordable fast offsite storage.

No Lock-In: Migrate backups from one cloud to another with a simple transfer, all within Retrospect.

Zero-Knowledge Security: With AES-256 encryption in-transit and at-rest, only customers can access their backups, no matter where they store them.

Fast Upload: Retrospect can saturate any connection with multiple simultaneous backups or restores.

Every edition of Retrospect, from Solo to Multi Server, supports backing up to the following cloud services.

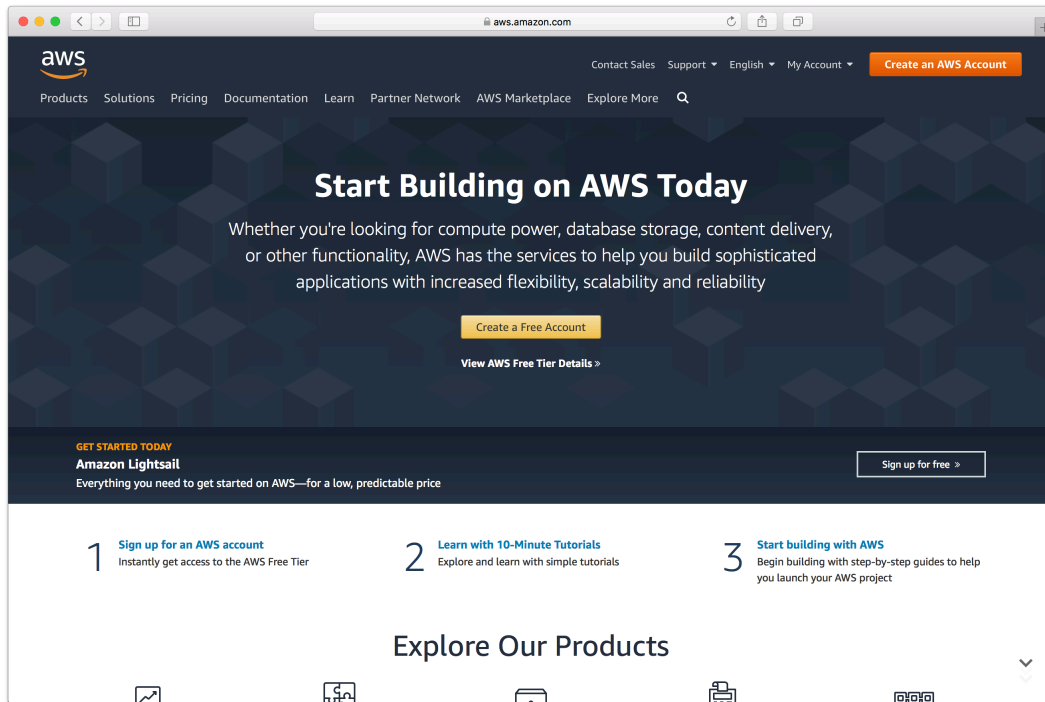
Below is a step-by-step guide for integrating Amazon S3 into your workflow. See our Knowledgebase for many more step-by-step guides to other cloud storage providers.

Amazon S3 Account Setup Guide

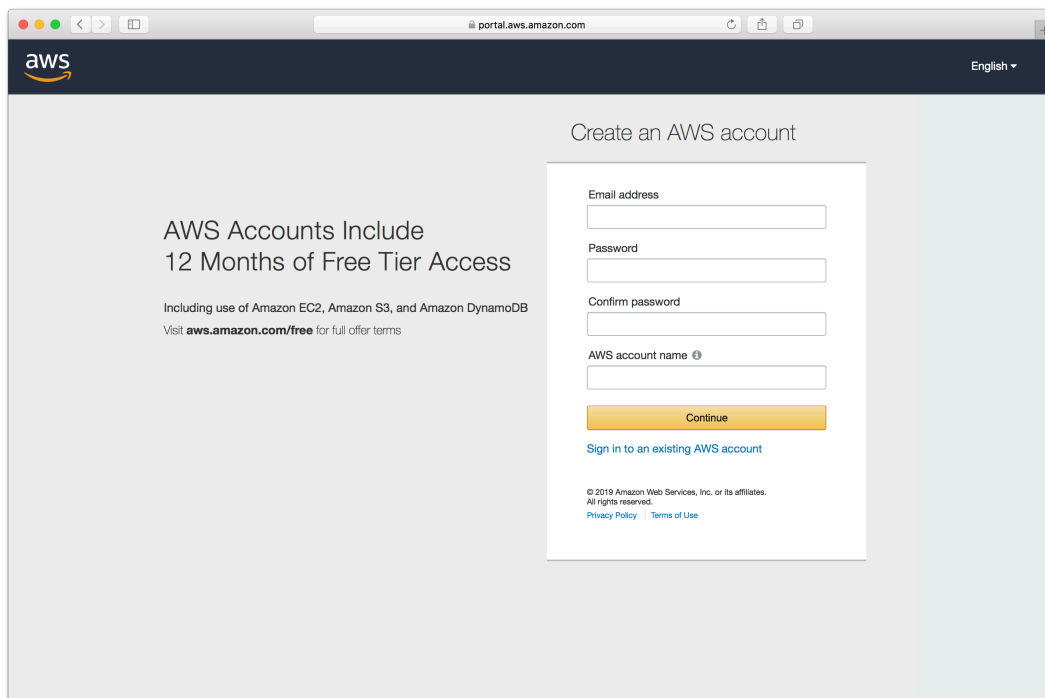
[Amazon S3](#) provides a low-cost, scalable cloud storage location for secure off-site data protection. It offers a [free tier](#) to its cloud services that includes 5GB of storage for a year. Retrospect 11 and higher for Windows and Retrospect 13 and higher for Mac are certified for Amazon S3. Follow these step-by-step instructions for setting up an Amazon S3 account, configuring a storage location (called a "bucket"), and creating a set of security credentials (an Access Key and a Secret Key, similar to a username and password).

See the following video or the steps below to quickly create an Amazon AWS account.

Visit [Amazon AWS](#) to start the account creation process and click "Create an AWS Account".



Fill in an email address and password.



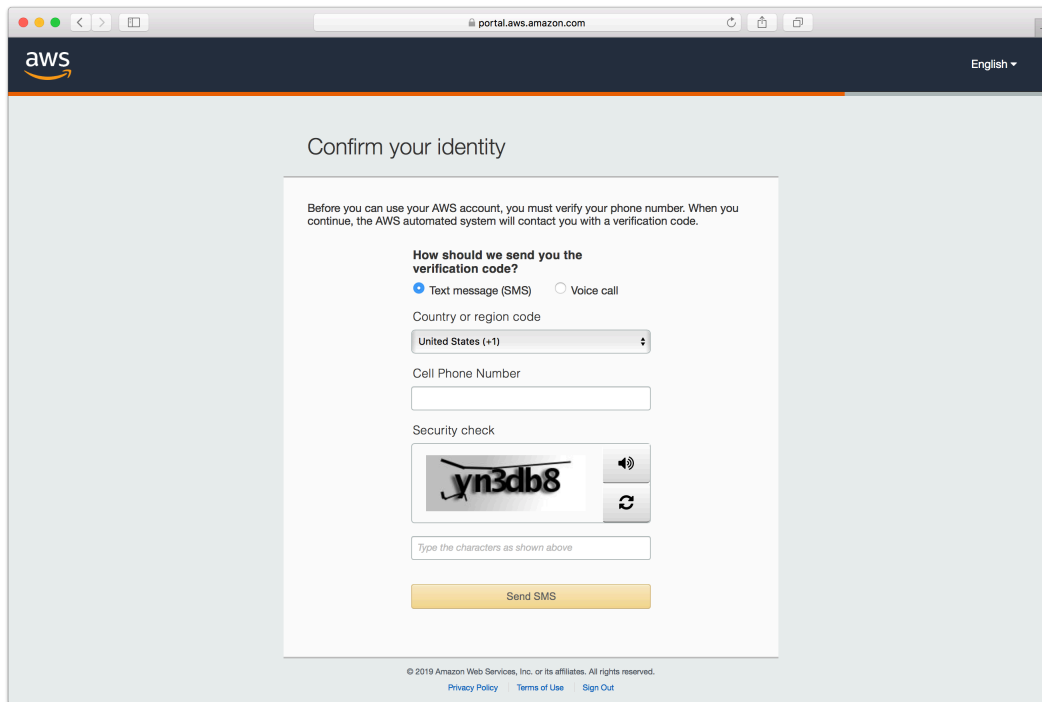
Complete the contact information form.

The screenshot shows a web browser window with the URL `portal.aws.amazon.com`. The page title is "Contact Information" and it includes the note "All fields are required." The form asks the user to "Please select the account type and complete the fields below with your contact details." The "Account type" section has two radio buttons: "Professional" (selected) and "Personal". Below this are input fields for "Full name", "Company name", and "Phone number". A "Country/Region" dropdown menu is set to "United States". The "Address" section has three input fields: "Street, P.O. Box, Company Name, c/o", "Apartment, suite, unit, building, floor, etc.", and "City". The "State / Province or region" field is also present.

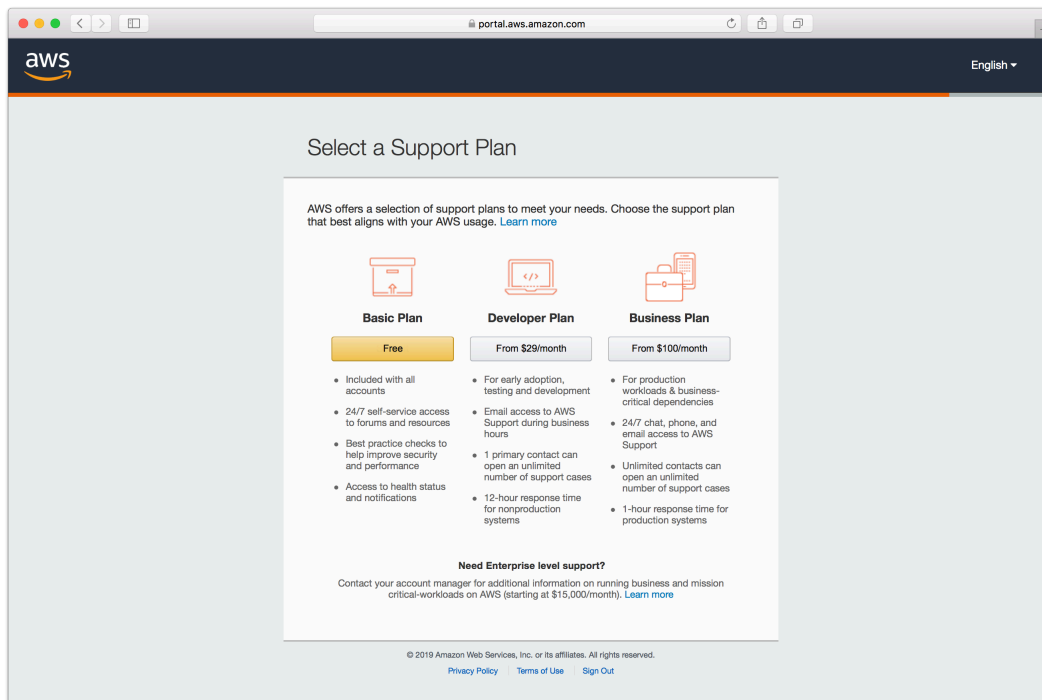
Complete the payment information form.

The screenshot shows a web browser window with the URL `portal.aws.amazon.com`. The page title is "Payment Information" and it includes the note "Please type your payment information so we can verify your identity. We will not charge you unless your usage exceeds the [AWS Free Tier Limits](#). Review [frequently asked questions](#) for more information." The form has input fields for "Credit/Debit card number" and "Cardholder's name". The "Expiration date" is set to "08" for the month and "2019" for the year. The "Billing address" section has two radio buttons: "Use my contact address" (selected) and "Use a new address". Below the selected option, the address is displayed as "1547 Palos Verdes Mall Suite 155", "Walnut Creek CA 94597", and "US". A yellow "Secure Submit" button is at the bottom of the form. At the very bottom of the page, there is a copyright notice: "© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved." with links for "Privacy Policy", "Terms of Use", and "Sign Out".

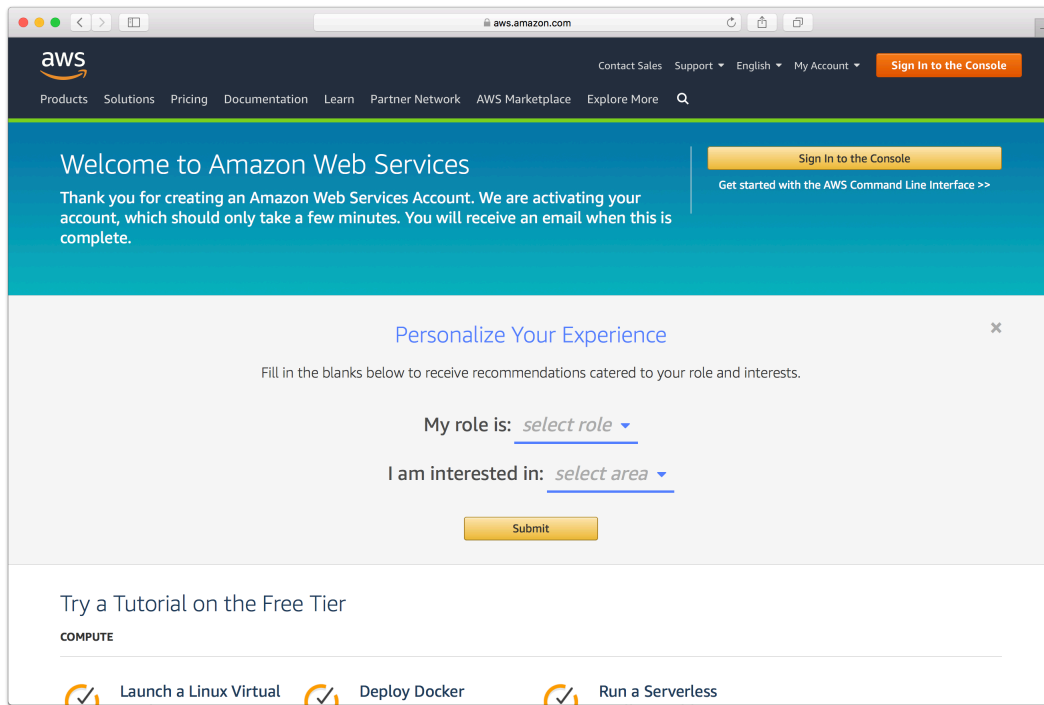
Complete the identity verification.



Select an appropriate Support Plan.



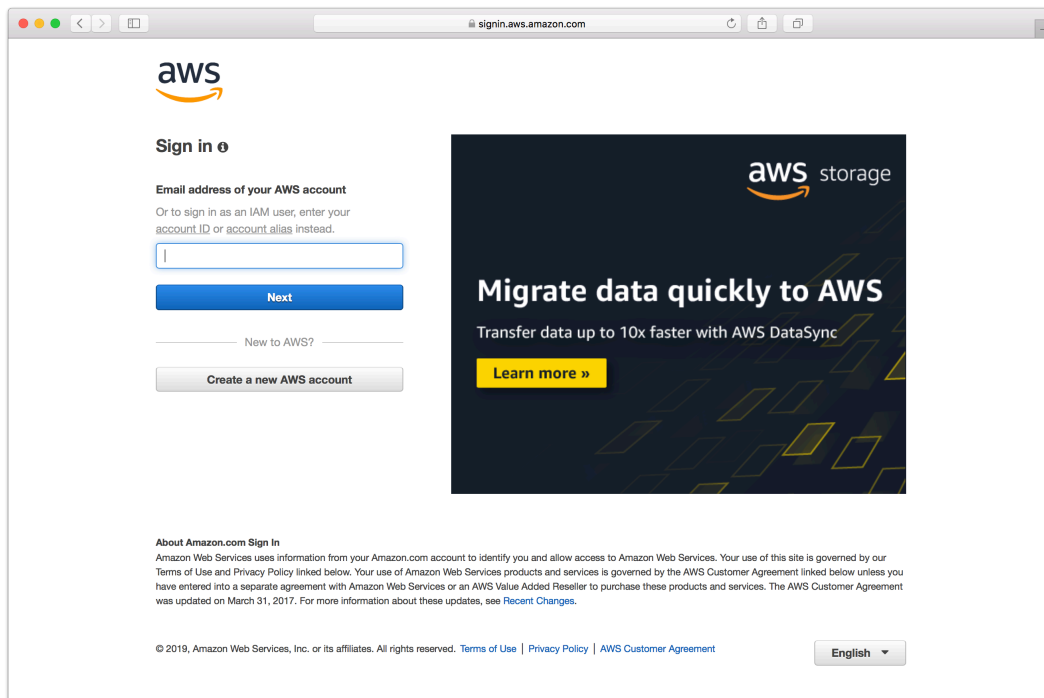
The new account is created. You're ready to set up the storage location.



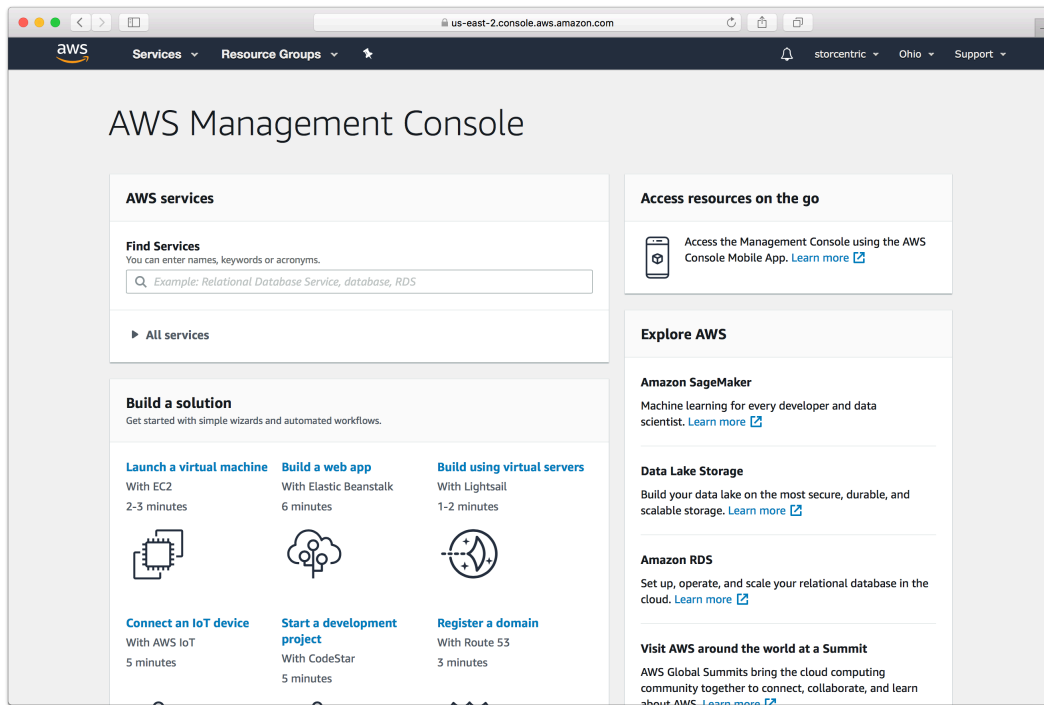
Storage Setup Guide

Now we will create a bucket that Retrospect can use to store backups.

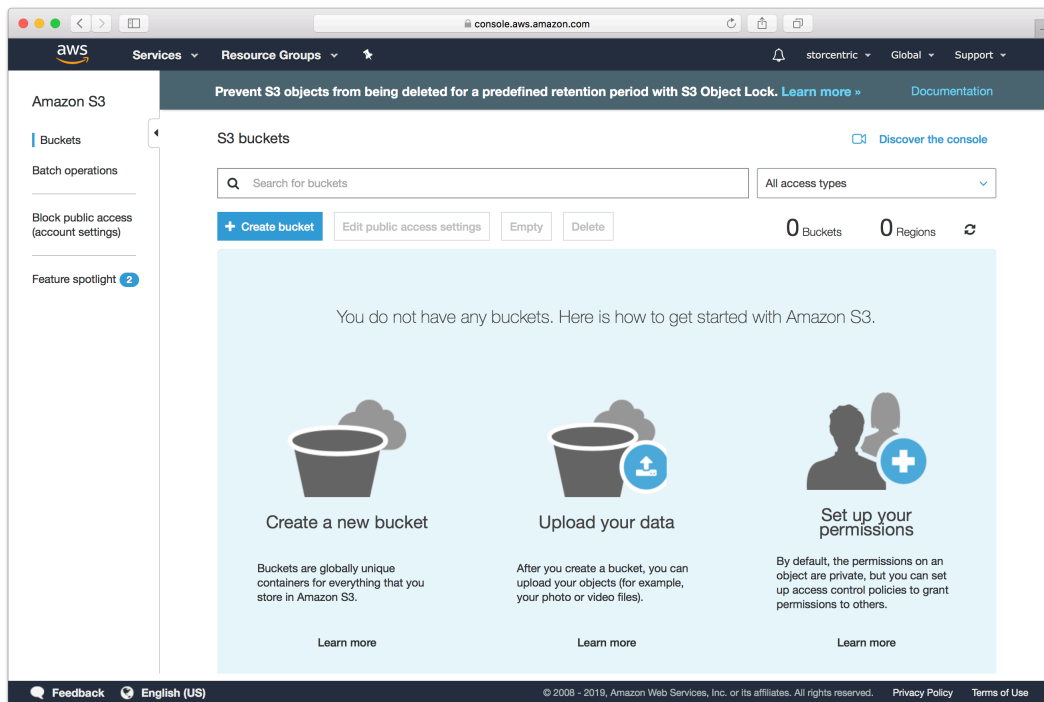
Log into AWS Console.



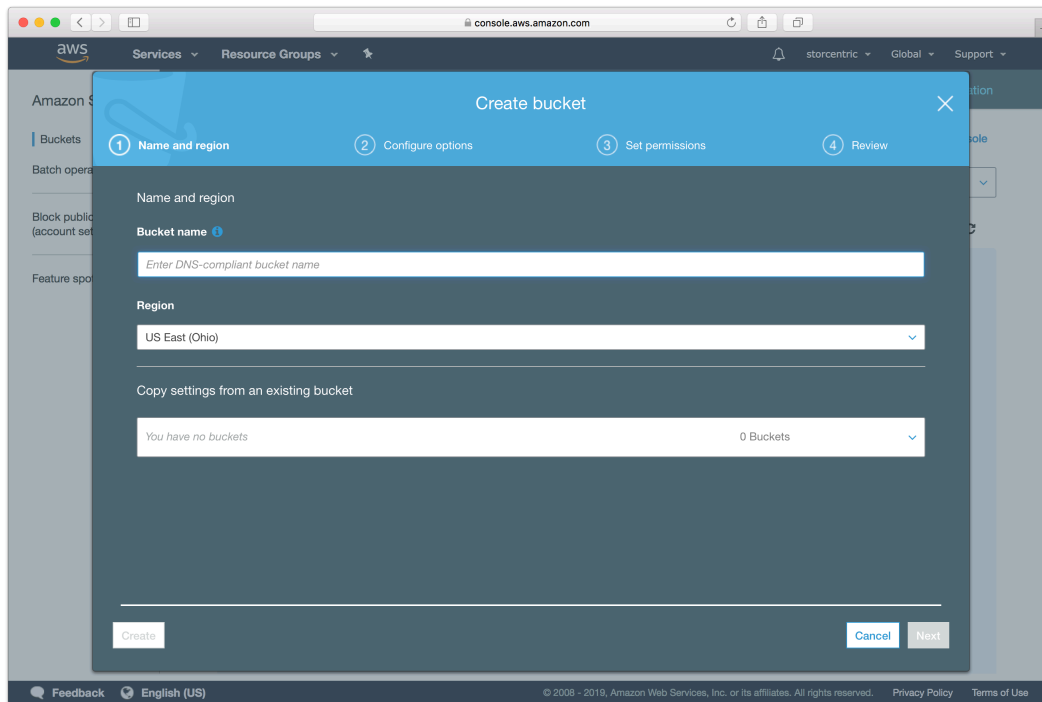
Search for S3 and select.



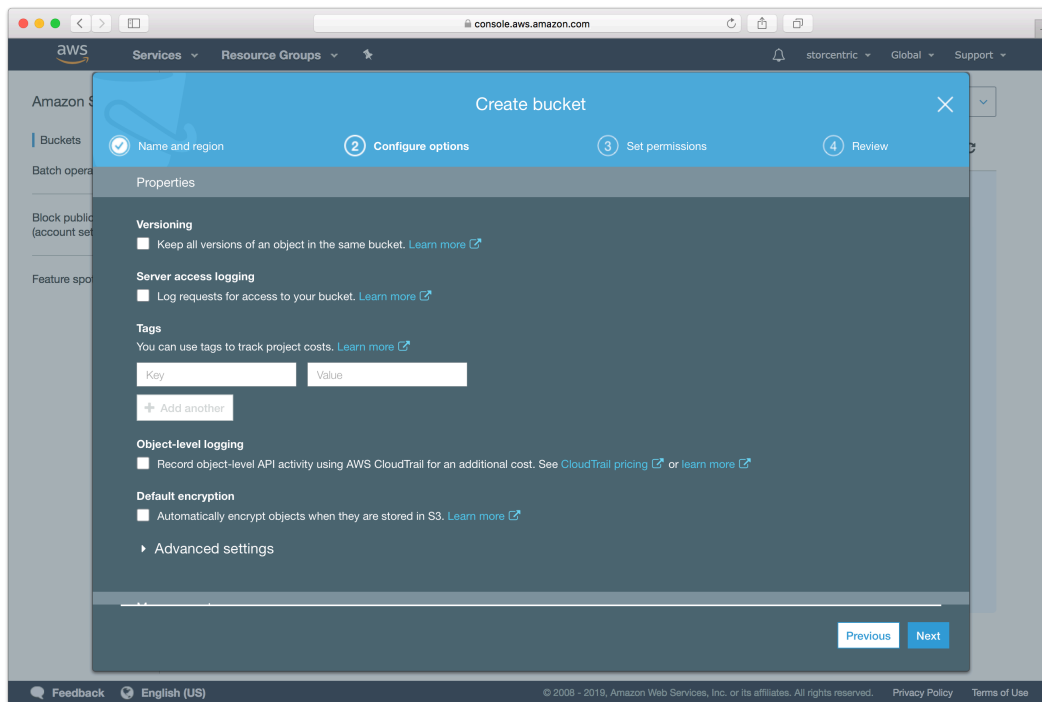
Click "Create Bucket".

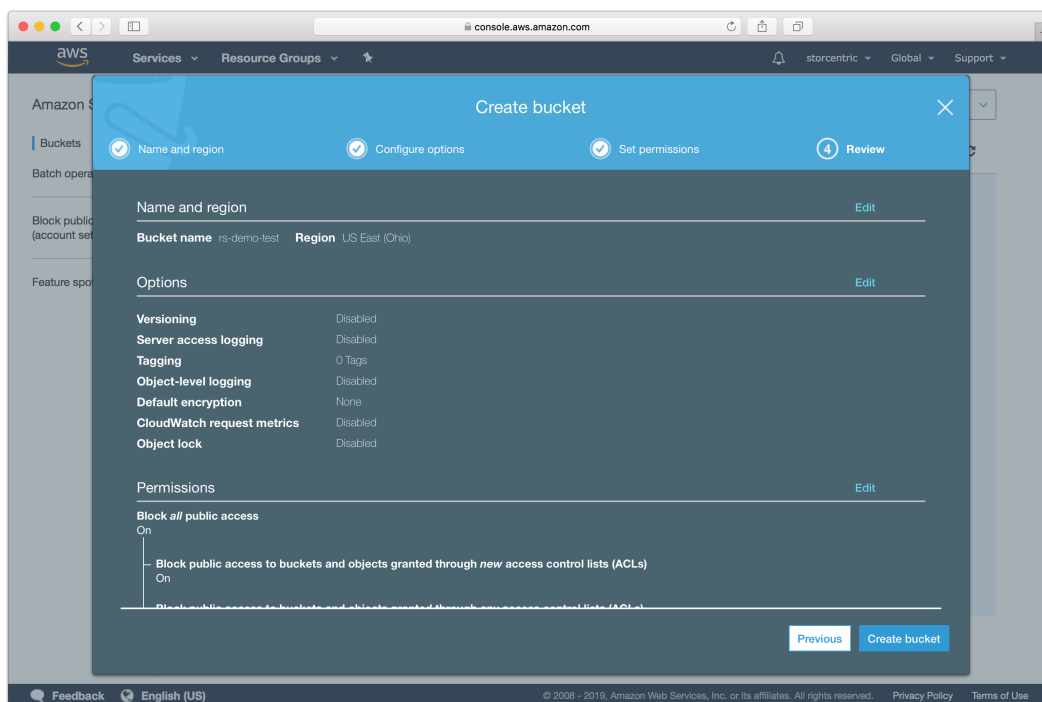
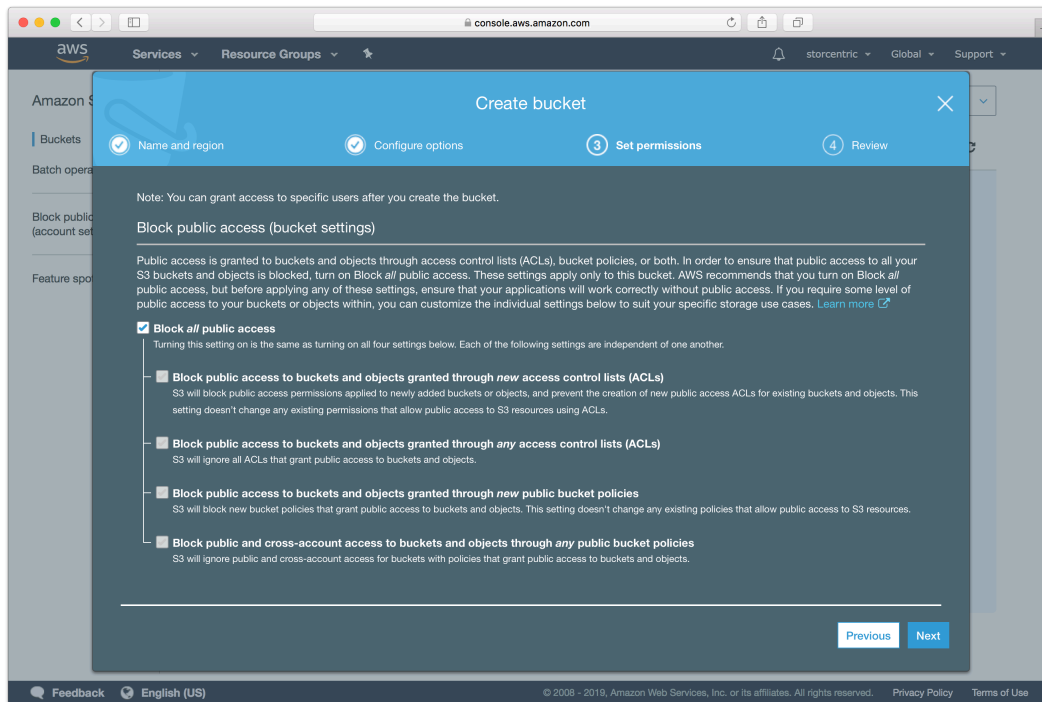


Type in an appropriate name for the bucket. Note that these are globally-unique names.

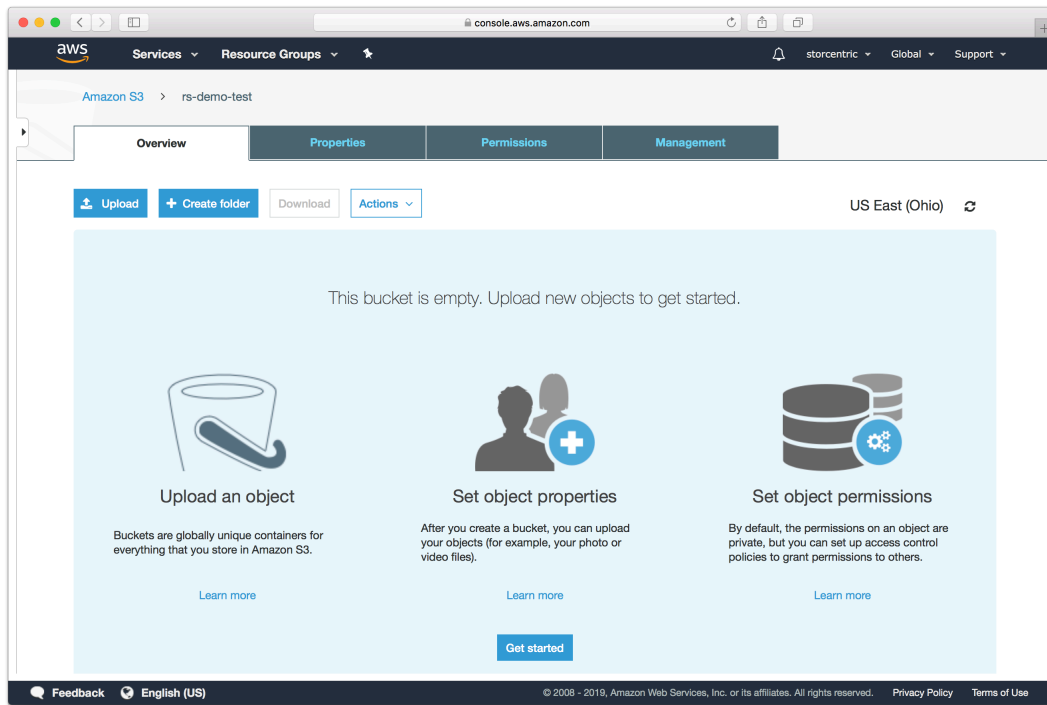


Continue through the rest of the wizard with default options.





Your bucket is now ready. In Retrospect, the "Path" is `s3.amazonaws.com/your_bucket_name`. Next, you need a set of security credentials for Retrospect to use to access it.



Choosing a Storage Class

Amazon S3 offers [different storage classes](#) to tailor its feature set and [pricing model](#) to different use cases. Retrospect supports "Standard", "Reduced Redundancy", "Infrequent Access", "One-Region", and "Glacier". The default storage class is "Standard". See below for how to use the other storage classes.

#== Using "Infrequent Access" Storage Class

You can use Amazon's guide to [Lifecycle Management](#) or follow the steps below.

Go to S3, select your Retrospect bucket, click on Properties, select Lifecycle, and click "Add Rule".

Bucket: [redacted]

Region: US Standard
Creation Date: Tue Feb 02 15:17:10 GMT+000 2016
Owner: admin

- ▶ Permissions
- ▶ Static Website Hosting
- ▶ Logging
- ▶ Events
- ▶ Versioning
- ▼ Lifecycle

You can manage the lifecycle of objects by using [Lifecycle rules](#). Lifecycle rules enable you to automatically transition objects to the [Standard - Infrequent Access](#) Storage Class, and/or archive objects to the [Glacier](#) Storage Class, and/or remove objects after a specified time period. Rules are applied to all the objects that share the specified prefix.

Versioning is not currently enabled on this bucket.

You can use Lifecycle rules to manage all versions of your objects. This includes both the Current version and Previous versions.

[+ Add rule](#)

Save **Cancel**

Choose the target for the rule. This must include your set.

Lifecycle Rules

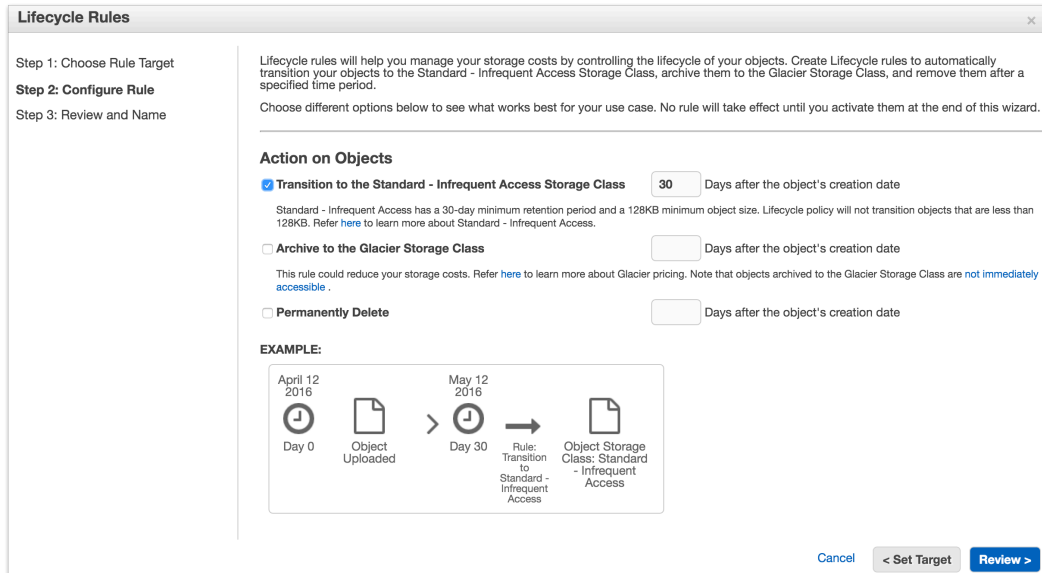
Step 1: Choose Rule Target
 Step 2: Configure Rule
 Step 3: Review and Name

Apply the Rule to: Whole Bucket: [redacted]
 A Prefix:

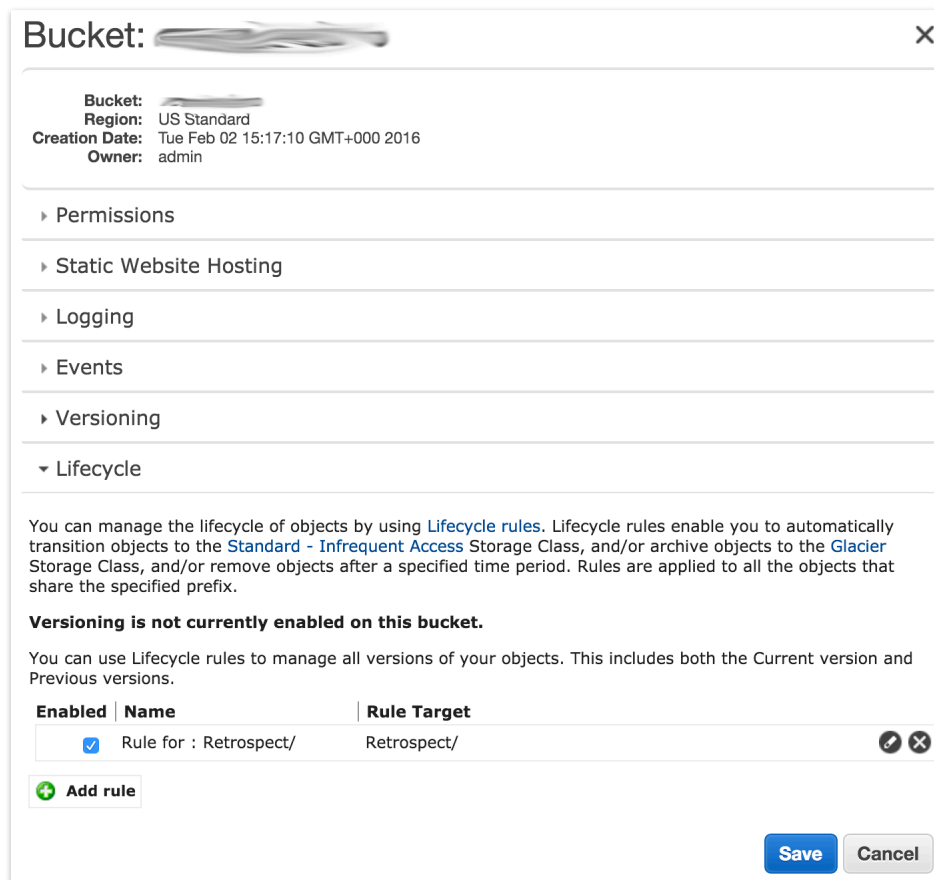
- Case sensitive. e.g. MyFolder/ or MyFolder/MyObject
- Rule will apply to all the objects that start with the specified prefix
- Don't include the bucket name in the prefix

Cancel **Configure Rule >**

Select "Transition to the Standard - Infrequent Access Storage Class". The minimum number of days is 30. Click "Review" and then "Create and Activate Rule"



You will see the rule listed in your bucket's Properties under Lifecycle.



#== Using "Glacier" Storage Class

You can use Amazon's guide to [Lifecycle Management](#) or follow the steps below.

Go to S3, select your Retrospect bucket, click on Properties, select Lifecycle, and click "Add Rule".

Bucket: [redacted]

Region: US Stanbard
Creation Date: Tue Feb 02 15:17:10 GMT+000 2016
Owner: admin

- ▶ Permissions
- ▶ Static Website Hosting
- ▶ Logging
- ▶ Events
- ▶ Versioning
- ▼ Lifecycle

You can manage the lifecycle of objects by using [Lifecycle rules](#). Lifecycle rules enable you to automatically transition objects to the [Standard - Infrequent Access](#) Storage Class, and/or archive objects to the [Glacier](#) Storage Class, and/or remove objects after a specified time period. Rules are applied to all the objects that share the specified prefix.

Versioning is not currently enabled on this bucket.

You can use Lifecycle rules to manage all versions of your objects. This includes both the Current version and Previous versions.

[+ Add rule](#)

Save **Cancel**

Choose the target for the rule. This must include your set.

Lifecycle Rules

Step 1: Choose Rule Target
 Step 2: Configure Rule
 Step 3: Review and Name

Apply the Rule to: Whole Bucket: [redacted]
 A Prefix: Retrospect/

- Case sensitive. e.g. MyFolder/ or MyFolder/MyObject
- Rule will apply to all the objects that start with the specified prefix
- Don't include the bucket name in the prefix

Cancel **Configure Rule >**

Select "Archive to the Glacier Storage Class". The minimum number of days is 1. Click "Review" and then "Create and Activate Rule"

Lifecycle Rules

Step 1: Choose Rule Target
Step 2: Configure Rule
 Step 3: Review and Name

Lifecycle rules will help you manage your storage costs by controlling the lifecycle of your objects. Create Lifecycle rules to automatically transition your objects to the Standard - Infrequent Access Storage Class, archive them to the Glacier Storage Class, and remove them after a specified time period.

Choose different options below to see what works best for your use case. No rule will take effect until you activate them at the end of this wizard.

Action on Objects

Transition to the Standard - Infrequent Access Storage Class Days after the object's creation date

Standard - Infrequent Access has a 30-day minimum retention period and a 128KB minimum object size. Lifecycle policy will not transition objects that are less than 128KB. Refer [here](#) to learn more about Standard - Infrequent Access.

Archive to the Glacier Storage Class Days after the object's creation date

This rule could reduce your storage costs. Refer [here](#) to learn more about Glacier pricing. Note that objects archived to the Glacier Storage Class are **not immediately accessible**.

Permanently Delete Days after the object's creation date

EXAMPLE:

Action on Incomplete Multipart Uploads

Cancel < Set Target Review >

You will see the rule listed in your bucket's Properties under Lifecycle.

Bucket: [redacted]

Bucket: [redacted]
Region: US Standard
Creation Date: Tue Feb 02 15:17:10 GMT+000 2016
Owner: admin

- ▶ Permissions
- ▶ Static Website Hosting
- ▶ Logging
- ▶ Events
- ▶ Versioning
- ▼ Lifecycle

You can manage the lifecycle of objects by using [Lifecycle rules](#). Lifecycle rules enable you to automatically transition objects to the [Standard - Infrequent Access](#) Storage Class, and/or archive objects to the [Glacier](#) Storage Class, and/or remove objects after a specified time period. Rules are applied to all the objects that share the specified prefix.

Versioning is not currently enabled on this bucket.

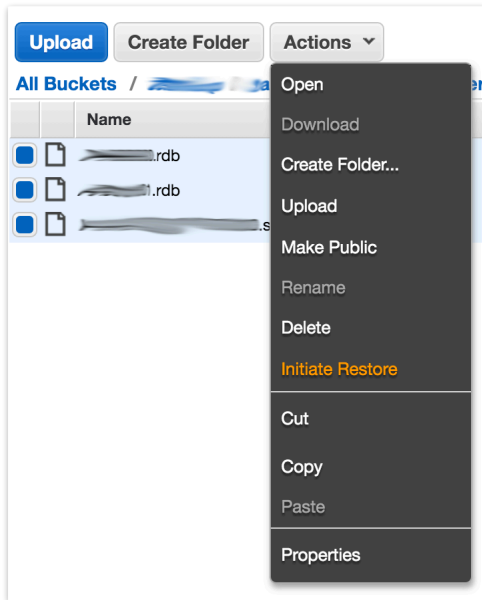
You can use Lifecycle rules to manage all versions of your objects. This includes both the Current version and Previous versions.

Enabled	Name	Rule Target
<input checked="" type="checkbox"/>	Rule for : Retrospect/	Retrospect/

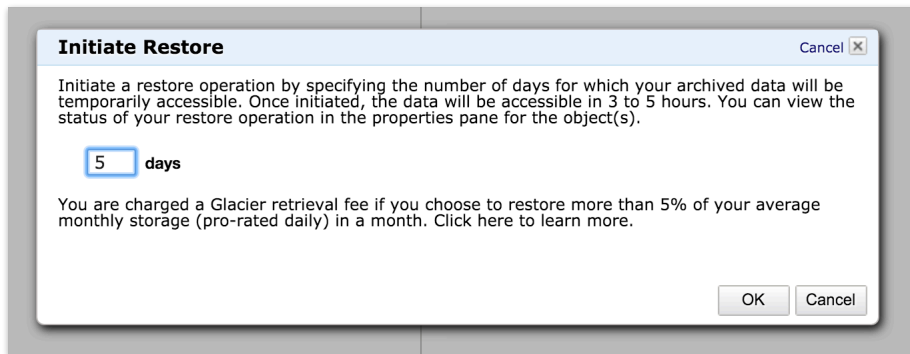
[Add rule](#)

Save Cancel

Files stored on Glacier require a separate restore process before Retrospect can access them. You need to select the files in the set and click "Initiate Restore".



Select the number of days you need to files temporarily available. The Glacier restore will start, and the set will be available for Retrospect within a few hours. You can see verify what storage class the set is by looking at the file browser.



#== Using "Reduced Redundancy" Storage Class

The "Reduced Redundancy" storage class is not available in Lifecycle. You must set this storage class periodically after a backup. You can use the AWS Console or a third-party tool like Cyberduck.

Go to S3, select your Retrospect bucket, navigate to your set, click on Properties, select "Reduced Redundancy, and click "Save".

Folder: [redacted]

Bucket Name: [redacted]

▼ Details

For all selected items:

Storage Class: Standard Standard - Infrequent Access Reduced Redundancy
Reduced redundancy storage will now be used

Server Side Encryption: None AES-256
Existing values will remain unchanged

Save Cancel

Simple Access Setup Guide

Now we will create the security credentials it can use to access that bucket. To grant Retrospect more granular access to your S3 account, please see the [Advanced Access Setup Guide](#).

Open the IAM console.

In the navigation pane, choose Users.

Choose your IAM user name (not the check box).

Choose the Security Credentials tab and then choose Create Access Key.

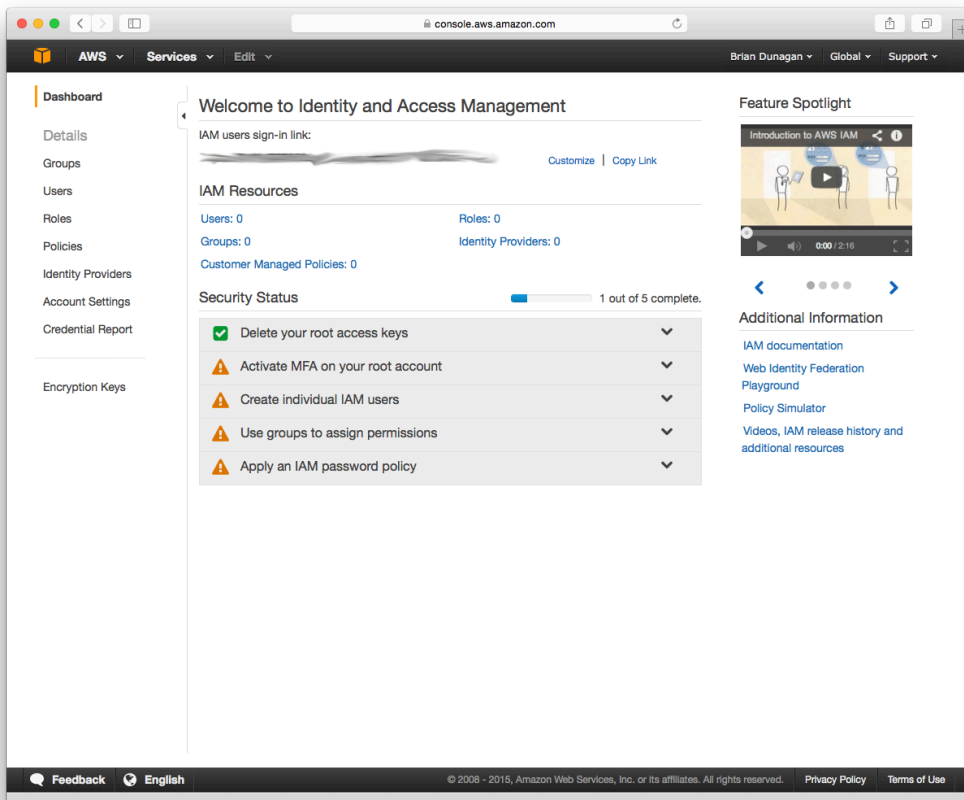
To see your access key, choose Show User Security Credentials. Your credentials will look something like this:

```
Access Key ID: AKIAI0SF0DNN7EXAMPLE
Secret Access Key: wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

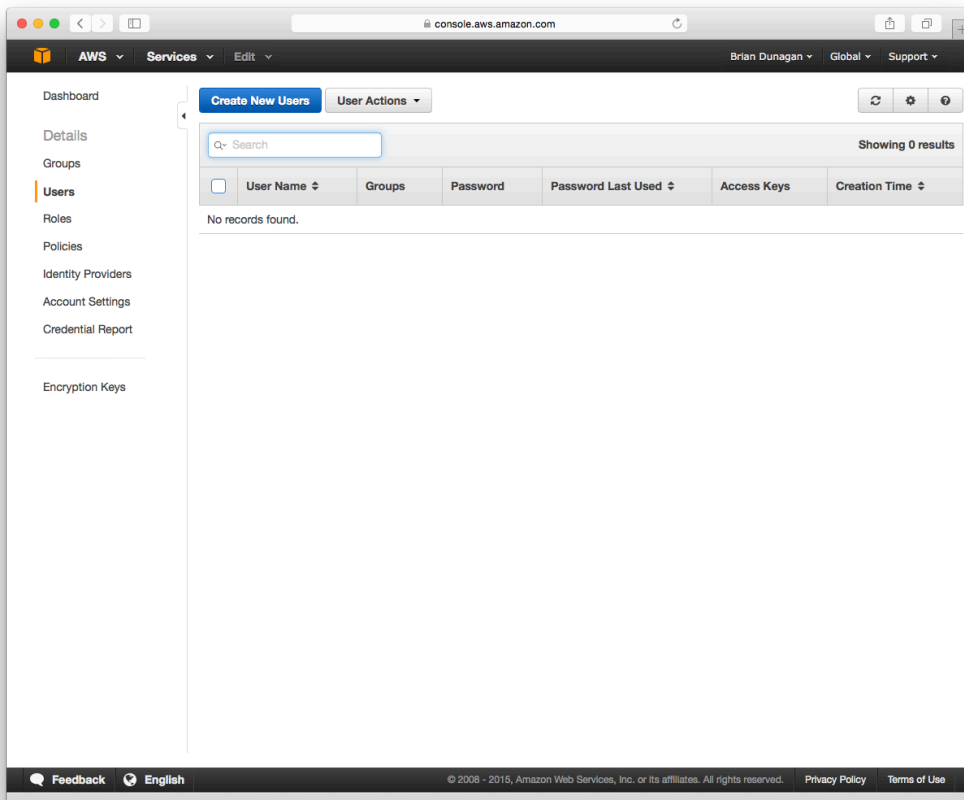
Choose Download Credentials, and store the keys in a secure location. Note that your secret key will no longer be available through the AWS Management Console; you will have the only copy. Keep it confidential in order to protect your account, and never email it. Do not share it outside your organization, even if an inquiry appears to come from AWS or Amazon.com. No one who legitimately represents Amazon will ever ask you for your secret key.

Advanced Access Setup Guide

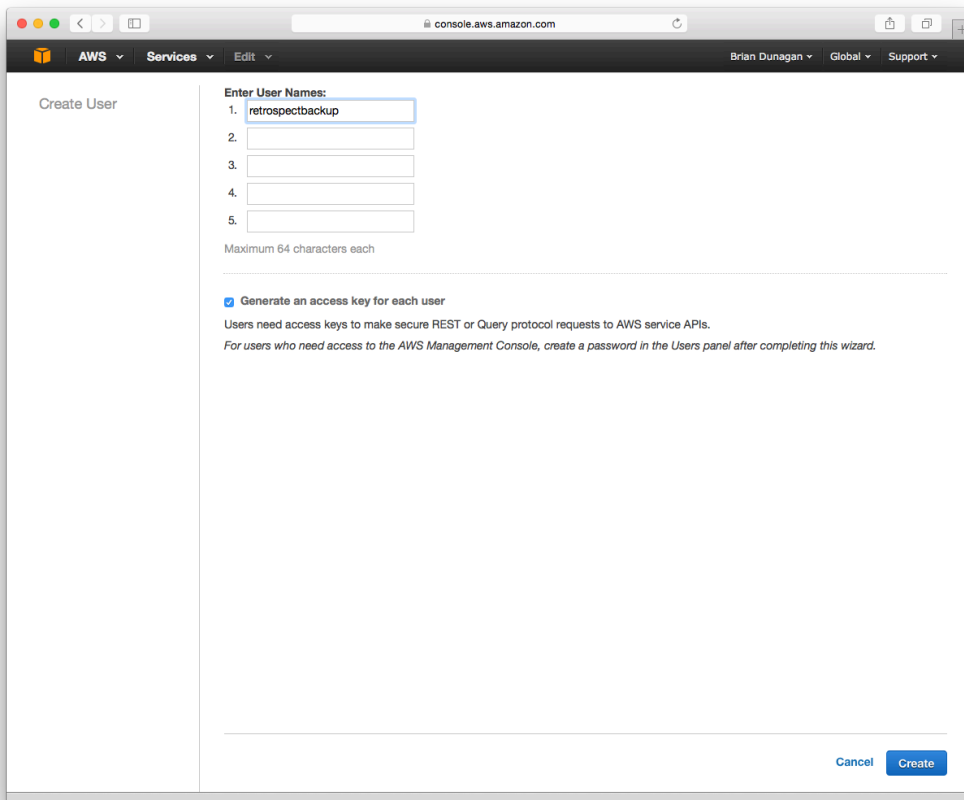
Go to IAM and click on "Users".



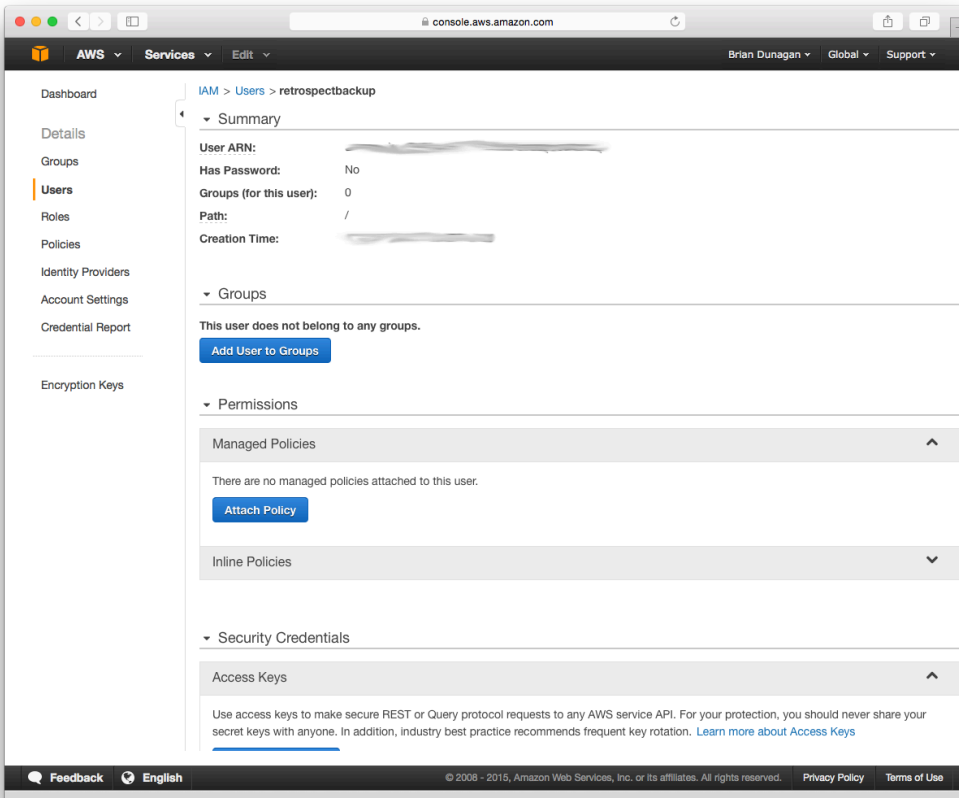
Click on "Create New Users".



Type in an appropriate username for Retrospect and click "Create". AWS will show you a set of credentials: an Access Key and a Secret Key. This is the only time AWS will show these, so download them to a safe place.



On the new user's account, click "Inline Policy" and then "Create User Policy". We are going to restrict this user's access to only the bucket we just created.



Choose "Custom Policy" and click "Select". Enter the following policy, replacing "your_bucket_name" with the name of the bucket you created.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::your_bucket_name",
        "arn:aws:s3:::your_bucket_name/*"
      ]
    }
  ]
}
```

When you're done, click "Validate Policy" then "Apply Policy". With this, Retrospect will have full access to that bucket but no access to anything else on S3 or other AWS services.

Information for Retrospect

Retrospect needs three pieces of information to access Amazon S3:

Path – `s3.amazonaws.com/your_bucket_name`

Access Key – Use the Access Key from above.

Secret Key – Use the Secret Key from above.

For the path, Amazon S3 supports different paths for its regions. Please see the following paths for the region you specified when creating the bucket:

Ireland – `s3-eu-west-1.amazonaws.com/your_bucket_name`

Sydney – `s3-ap-southeast-2.amazonaws.com/your_bucket_name`

Singapore – `s3-ap-southeast-1.amazonaws.com/your_bucket_name`

Tokyo – `s3-ap-northeast-1.amazonaws.com/your_bucket_name`

Sao Paulo – `s3-sa-east-1.amazonaws.com/your_bucket_name`

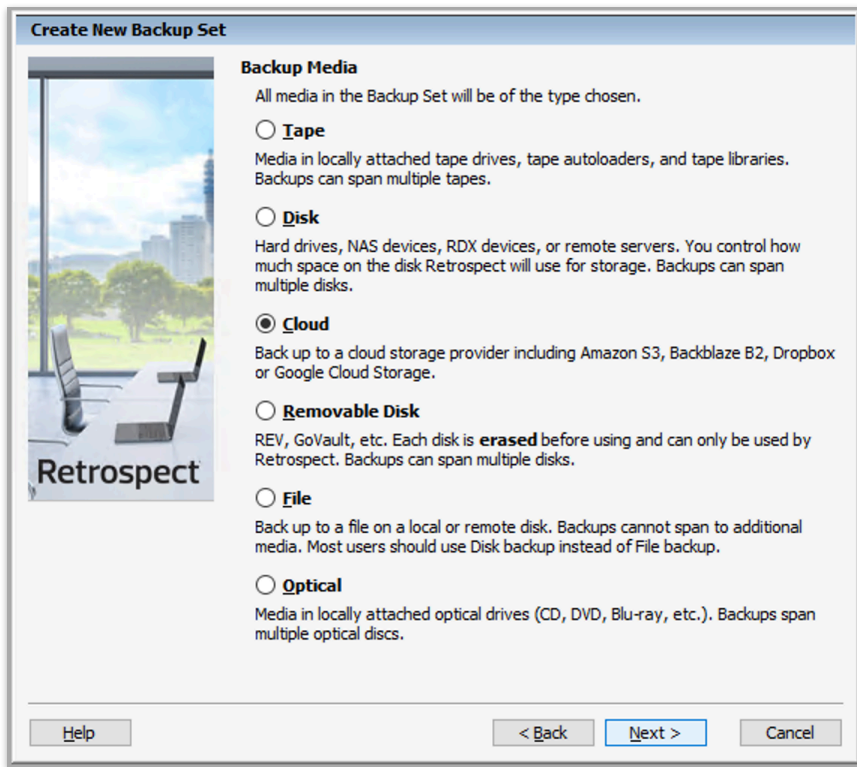
See [Amazon S3 Regions/Endpoints](#) for further details.

Note that if you use the default path of `s3.amazonaws.com` for a region outside of the United States, you may receive the following error: "These credentials are not valid". Please use the region-specific URL above to correct this.

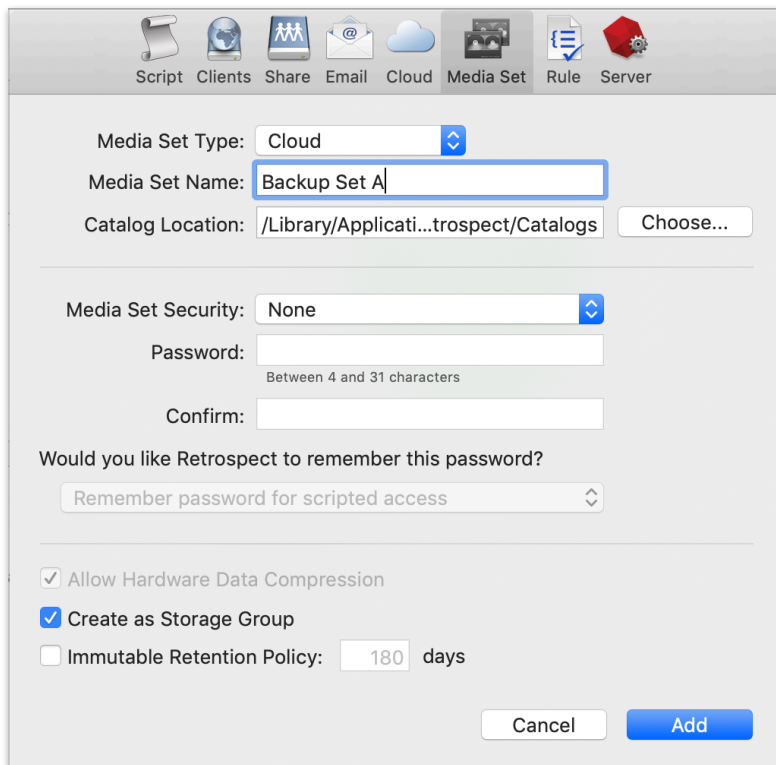
Adding Cloud Storage in Retrospect

Adding cloud storage as a destination is simple. Retrospect has a new set type called "Cloud". Create a new backup set/media set and select "Cloud" as the type.

Windows Interface



Mac Interface



Next you'll need to enter your cloud storage credentials. Retrospect allows customers to enable or disable SSL encryption (HTTP or HTTPS) and to set the maximum storage usage, up to 8TB per cloud member.

Windows Interface

Create New Backup Set

Cloud Backup Set
Enter a Backup Set name and set up cloud storage.
Once the Backup Set has been created the name cannot be changed.

Member Type: Amazon S3 compatible

Name: S3 Backup Set

Path:

Access Key:

Secret Key:

Use SSL

[Learn how to set up a cloud storage account](#)

Use at most: 8,192 GB

Help < Back Next > Cancel

Mac Interface

Member Type: Cloud Storage

[Learn how to set up a cloud storage account](#)

Path: s3.amazonaws.com/bucketName

Access Key:

Secret Key:

Use SSL

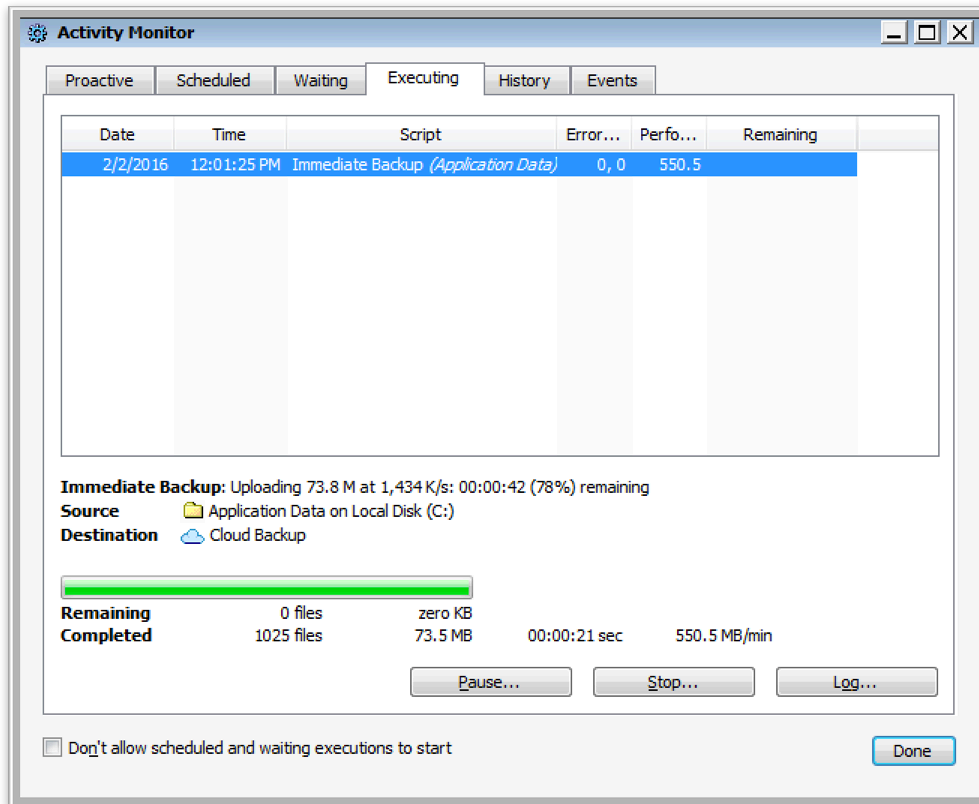
Use at most: 4096 GB

Cancel Add

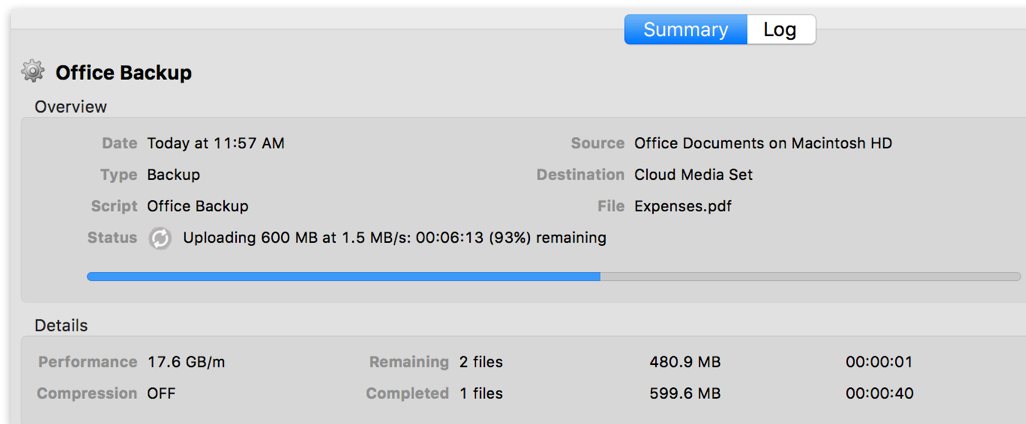
Using Cloud Storage in Retrospect

Using cloud storage is simple. After you have created a cloud set, create a new script or add it to an existing one, and click "Run". The backup will begin with the contents of the set being uploaded to your cloud storage location. You can track the progress in the execution/activity.

Windows Interface



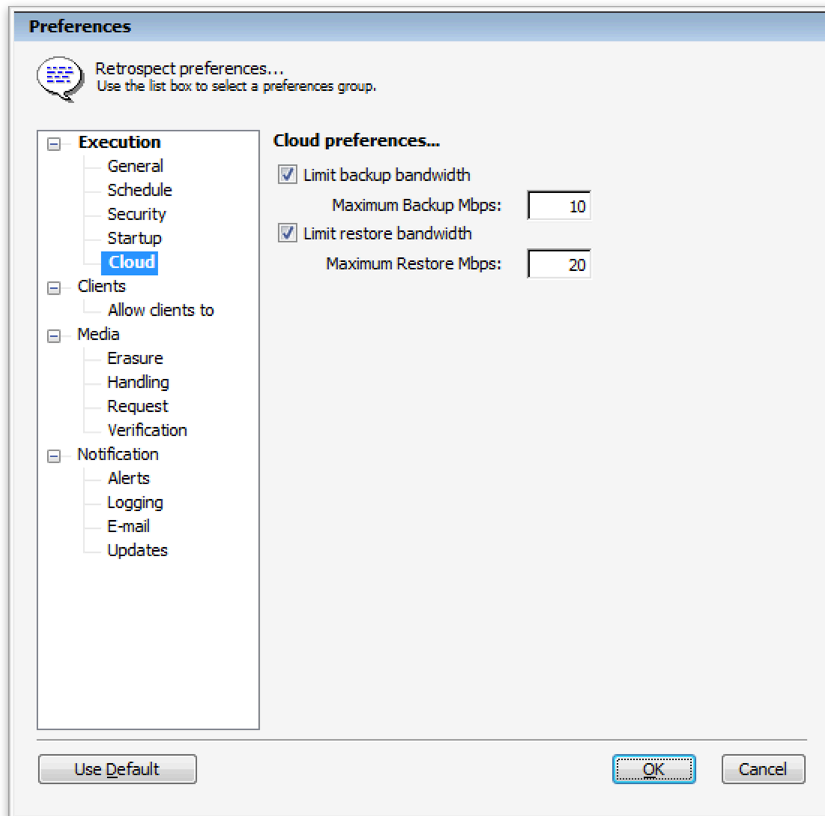
Mac Interface



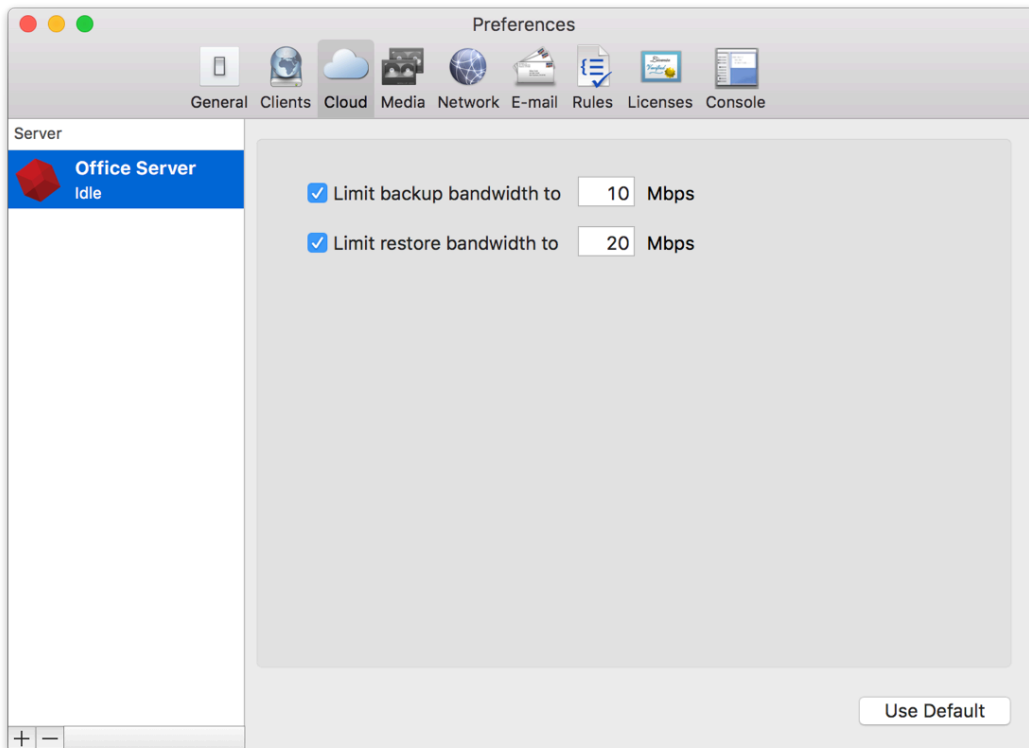
Throttling Cloud Backups in Retrospect

Throttling for cloud backup and cloud restore is available in Preferences.

Windows Interface



Mac Interface



General Tips

Below are a number of tips for using cloud storage in Retrospect:

Bandwidth Measurement Tool – Measure your upload and download bandwidth with this free tool: [Speedtest.net](https://www.speedtest.net).

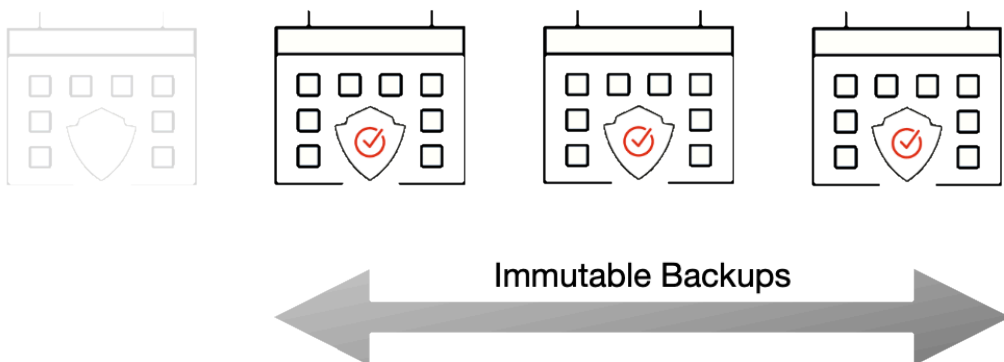
Disable Backup Verification – Verification will download all of the data that you upload. See more details about why you should disable it for cloud backups in [Cloud Backup – Best Practices for Data Protection with Cloud Storage](#).

Ransomware Protection

Overview

Ransomware attacks are increasingly sophisticated, having the capability of watching for cloud account credentials, deleting backups and cloud storage, then encrypting everything and demanding a ransom. It's imperative to build defenses against this escalating attack. SMBs and large businesses need a backup target that allows them to lock backups for a designated time period. Many of the major cloud providers now support object locking, also referred to as Write-Once-Read-Many (WORM) storage or immutable storage. Users can mark objects as locked for a designated period of time, preventing them from being deleted or altered by any user.

Retrospect Backup integrates seamlessly with this new object lock feature. Users can set a retention period for backups stored on supporting cloud platforms. Within this immutable retention period, backups cannot be deleted by any user, even if ransomware or a malicious actor acquires the root credentials. Retrospect Backup's powerful policy-based scheduling allows it to predict when those backups will leave the retention policy and protect any files that will no longer be retained, ensuring businesses always have point-in-time backups to restore within the immutable retention policy window.



Retrospect provides immutable backup protection with Amazon S3, Microsoft Azure, Google Cloud, Backblaze B2, Wasabi, and MinIO. Below is a step-by-step guide to using Amazon S3 for immutable backups.

For more information about backing up to Amazon S3 with Retrospect Backup, see [How to Set Up an Amazon S3 Account](#). For more information about other cloud providers, see [Cloud Backup](#).

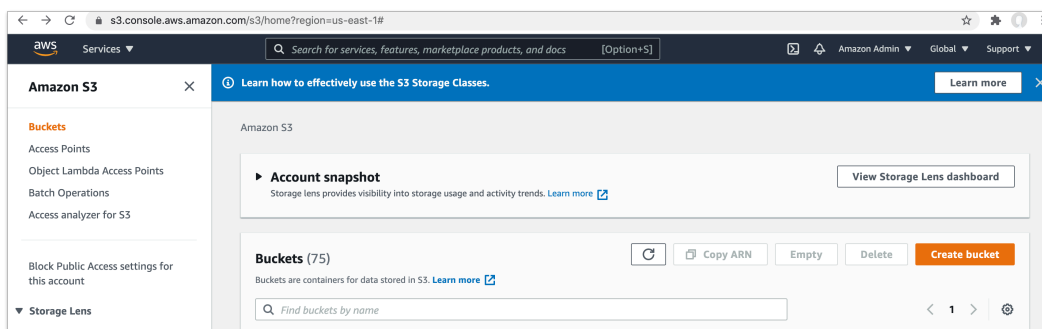
Step-by-Step Guide

Retrospect Backup makes it easy to add an immutable retention policy with Amazon S3. When creating a backup set, simply check "Immutable Retention Policy" and specify the number of days. Retrospect Backup will mark any backups to Amazon S3 as immutable until that date in the future and delete any backups that are no longer protected by the retention policy, saving costs on storage space.

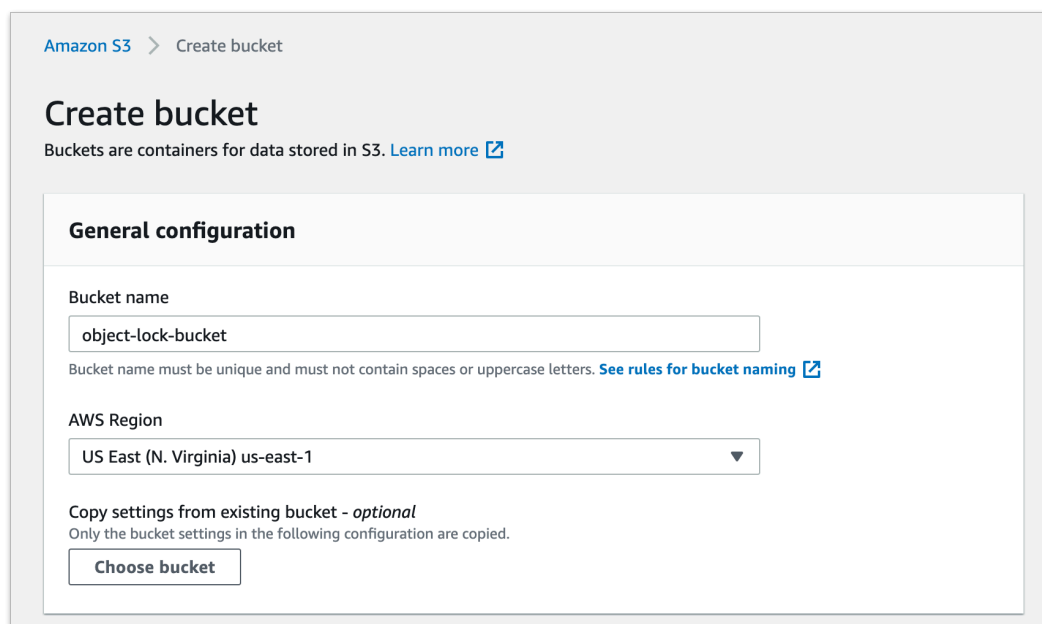
Let's walk through the steps to create an immutable backup.

Amazon S3: [Create an account on Amazon S3](#) if you have not already.

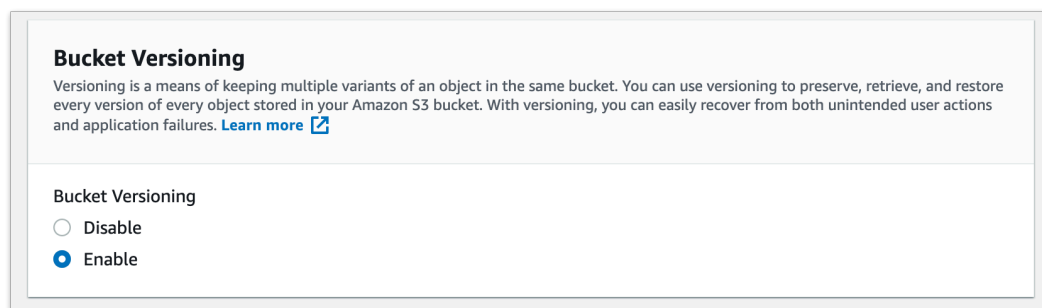
Amazon S3: Click "Create Bucket".



Amazon S3: Enter a bucket name.



Amazon S3: Enable "Bucket Versioning". This option is required for Object Lock. It means S3 will store versions of each file, and to delete one, you need to delete every version of it.



Amazon S3: Enable "Object Lock" then click "Create Bucket". Enabling "Object Lock" does not

enforce a retention period. It simply allows Retrospect to add one to each file.

▼ **Advanced settings**

Object Lock
Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. [Learn more](#)

Disable

Enable
Permanently allows objects in this bucket to be locked. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten.

Object Lock works only in versioned buckets. Enabling Object Lock automatically enables Bucket Versioning.

⚠ Enabling Object Lock will permanently allow objects in this bucket to be locked
Enable Object Lock only if you need to prevent objects from being deleted to have data integrity and regulatory compliance. After you enable this feature, anyone with the appropriate permissions can put immutable objects in the bucket. You might be blocked from deleting the objects and the bucket. Additional Object Lock configuration is required in bucket details after bucket creation to protect objects in this bucket from being deleted or overwritten. [Learn more](#)

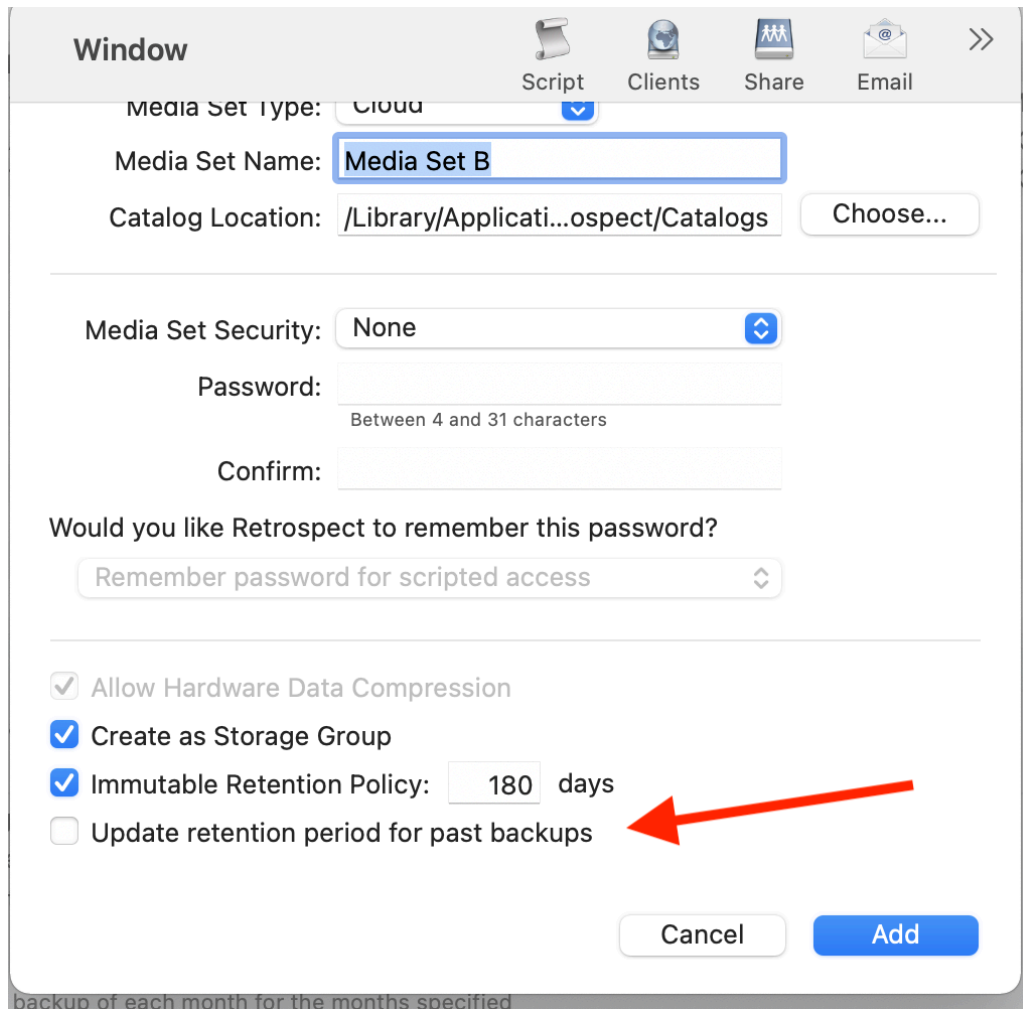
I acknowledge that enabling Object Lock will permanently allow objects in this bucket to be locked.

After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel **Create bucket**

Retrospect: Add a destination. On Windows, select "Backup Sets" then "Create". On Mac, select "Media Sets" and click "Add". Select type "Cloud". Then click "Immutable Retention Policy" and specify the number of days to protect your backups.

The default retention window is a rolling window, where backups exit the window and files are re-backed up. You can also choose an archival window, where immutable backups have their retention dates extended to not exit the window. Select "Update retention period for past backups".



Retrospect: Add the destination to a script, and set the script grooming policy to match the retention period. By ensuring the two time periods match, Retrospect Backup will automatically delete backups that fall outside of the retention policy.

Amazon S3: You can always verify the retention period of a file in AWS Management Console under the file's "Properties" tab in the "Object Lock" section.

Technical Details

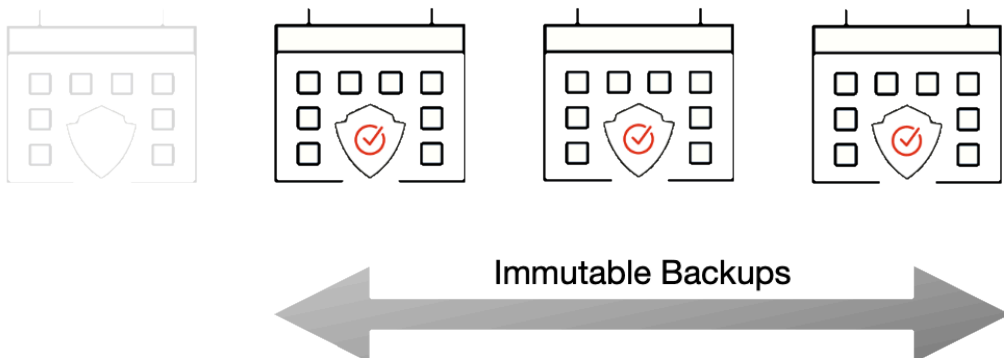
Every backup within the retention period is an immutable backup with point-in-time restore capabilities. Because each backup is incremental, Retrospect only transfers the files that are new or have changed since the last backup. However, you can always restore any part of a backup in Retrospect.

Retrospect Backup uses its advanced scheduling workflow to make sure every immutable backup includes all applicable files. Let's say the chosen retention period is 90 days, and backups occur every week. Retrospect Backup starts backing up. When it gets to Day 85, it looks ahead to the upcoming back on Day 92. There are two options for how to proceed:

Rolling Window: This default approach marks which files will no longer be protected on that date

based on when they were last backed up, and adds them to the new immutable backup.

Archival Window: Immutable backups have their retention dates extended to not exit the window. Select "Update retention period for past backups".



With the grooming policy set to match the retention policy, Retrospect will automatically delete the backups that are no longer immutable, saving you storage space while ensuring every file is protected by an immutable backup.

The maximum allowed retention period by Retrospect is 9,999 days.

Anomaly Detection

Overview

Ransomware is a huge global threat to businesses around the world. Businesses are projected to have paid out \$20B in 2021, a 100% Y-o-Y increase for the last four years, and it's only going to get worse with new business models like RaaS: ransomware-as-a-service. With Retrospect Backup, businesses can protect their infrastructure with immutable backups for ransomware protection.

Organizations need to detect ransomware as early as possible to stop the threat and remediate those resources. Anomaly Detection in Retrospect Backup identifies changes in an environment that warrants the attention of IT. Administrators can tailor anomaly detection to their business's specific systems using customizable filtering and thresholds for each of their backup policies, and those anomalies are aggregated on Retrospect Management Console across the entire business's Retrospect Backup instances or a partner's client base with a notification area for responding to those anomalies.

The key to detection is combining technologies such as signature detection in processes with file-based irregularities. Using a multi-pronged defense, with immutable backups, anomaly detection, and other security layers, businesses will know when they're being attacked and will have the tools to remediate it and move on.

Detecting Anomalies

Ransomware is now a vast ecosystem with many different forms of attacks. Many attackers have their own versions of ransomware, and these are called variants. Each variant has the same purpose, but it uses a different mechanism or simply a different naming convention. The majority of ransomware variants and all of the top 10 forms for 2021 followed the same attack pattern: infiltrate a computer and rename the files with a different extension.

The Most Common Ransomware Variants in Q3 2021

Rank	Ransomware Type	Market Share %	Change in Ranking from Q2 2021
1	Conti V2	19.2%	+1
2	Mespinoza	11.3%	+2
3	Sodinokibi	8.9%	-2
4	Lockbit 2.0	8.4%	New in Top Variants
5	Hello Kitty	5.4%	-
6	Zeppelin	4.4%	+3
7	Ranzy Locker	3.0%	New in Top Variants
8	Suncrypt	2.5%	New in Top Variants
8	Hive	2.5%	New in Top Variants
9	Ryuk	2.0%	-3
9	BlackMatter	2.0%	New in Top Variants

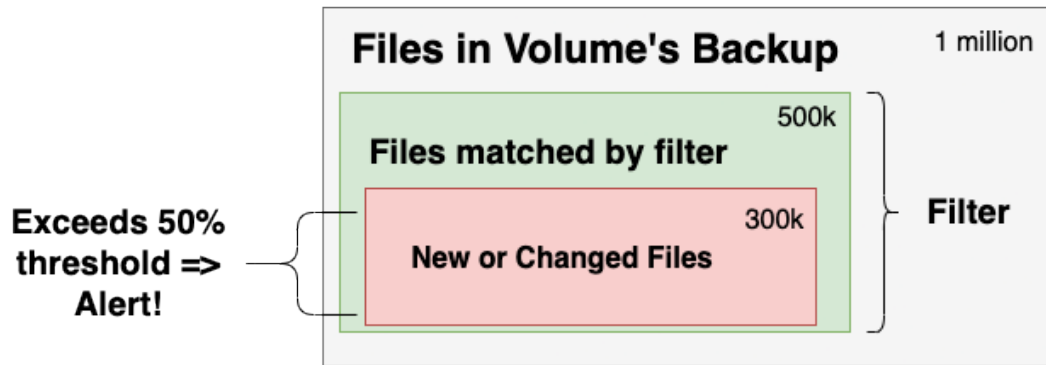
Top 10: Market Share of the Ransomware attacks

As a backup solution, Retrospect Backup has a significant footprint in a business's computer environment with visibility into endpoints, servers, NAS volumes, and even cloud storage. To detect anomalies, Retrospect Backup provides a per-policy option for filtering and threshold to decide whether or not certain file changes are an anomaly with options for notifications. Let's walk through each:

Filtering: Configure a filter to identify the files to observe. Retrospect lets administrators tailor this to file types, paths, dates, or specific attributes, and the built-in filter focuses on office documents, photos, and movies.

Threshold: Set the threshold for the alert. If the percentage of files new or changed out of the total number of files matched by the filter is greater or equal to the threshold, Retrospect will create an anomaly event.

Notification: Access notifications on Retrospect Management Console, receive them immediately in an email, and find them in the Execution History and Backup Report. Retrospect surfaces the notification for anomaly detection in the best place for an organization.



The diagram shows the volume being monitored as a whole, the subset of files that match the "Anomaly Detection" filter, and the files that are new or changed within that subset. Retrospect generates an alert if the percentage exceeds the threshold.

Step-by-Step Setup Guide

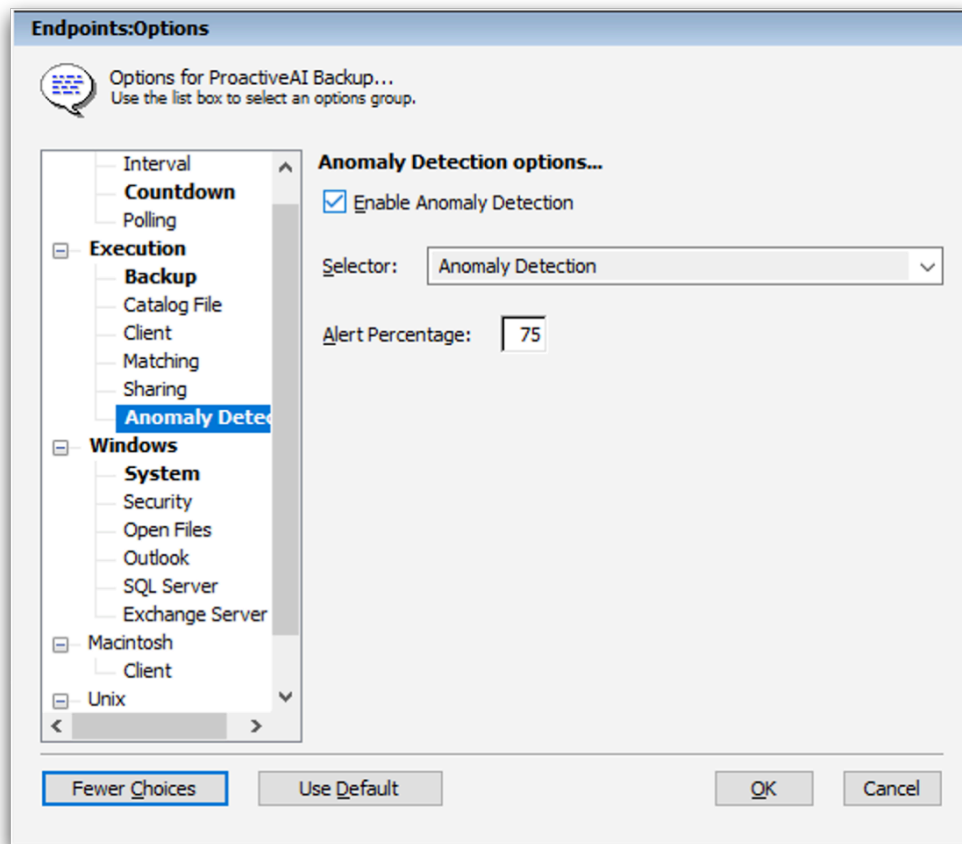
Let's walk through setting up Anomaly Detection for both Retrospect Backup for Windows and Retrospect Backup for Mac.

Launch Retrospect.

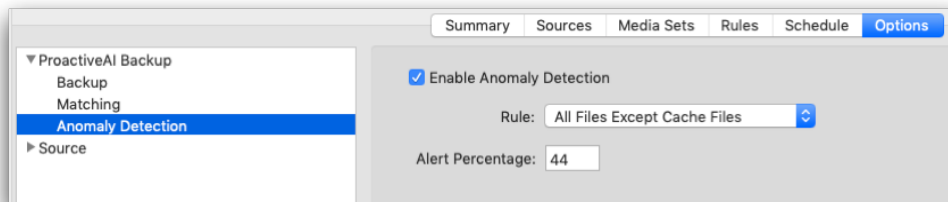
Open "Scripts" and select the policy you would like to change (or create a new one).

Note: Anomaly Detection is only supported for "Backup" and "ProactiveAI" script types. You cannot perform anomaly detection during a replication/duplicate/copy process.

Under "Options", click "Anomaly Detection".



Retrospect Backup for Windows



Retrospect Backup for Mac

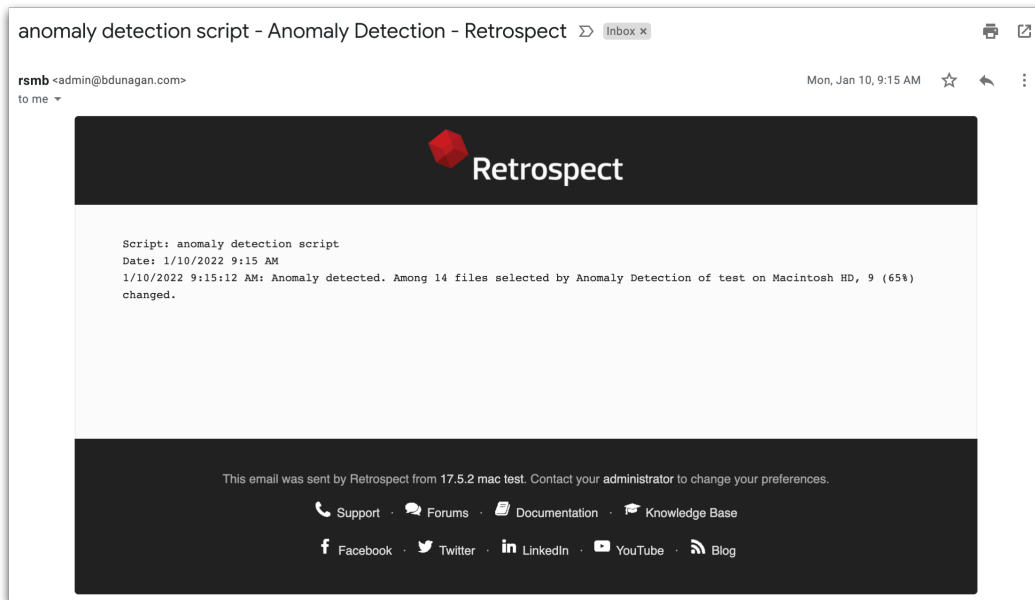
Click "Enable Anomaly Detection" to enable the feature.

Select the appropriate filter. These are called "Selectors" (Windows) or "Rules" (Mac). You can edit them under "Preferences".

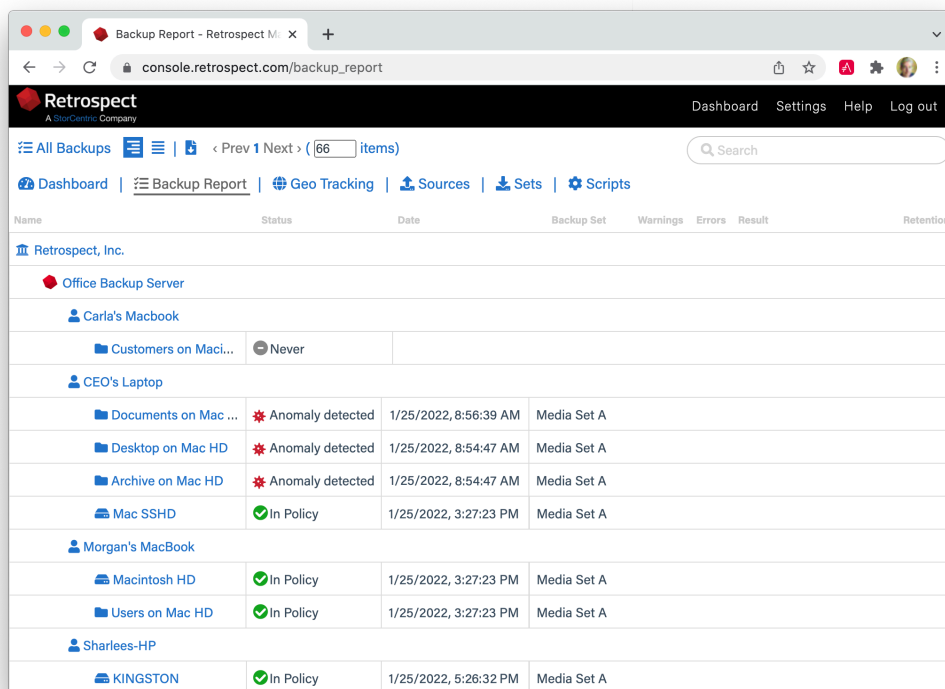
Set the appropriate threshold percentage.

Save the script.

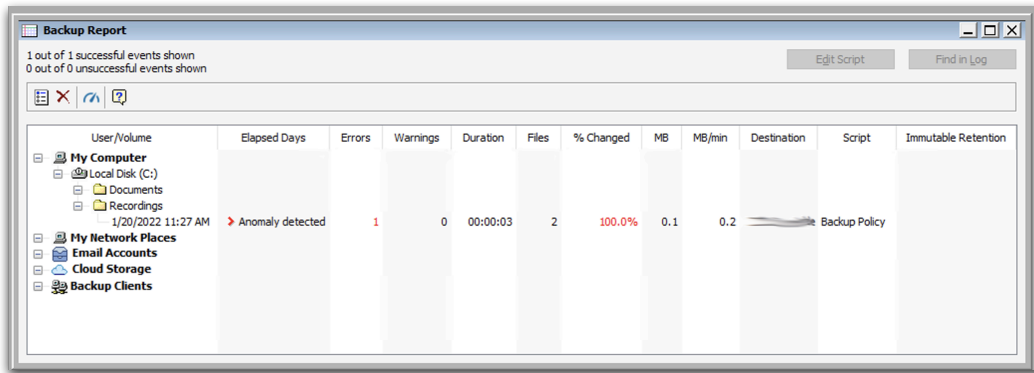
Anomaly Detection is now enabled for the volumes within that policy. If an anomaly is detected, you can find notifications in a number of locations:



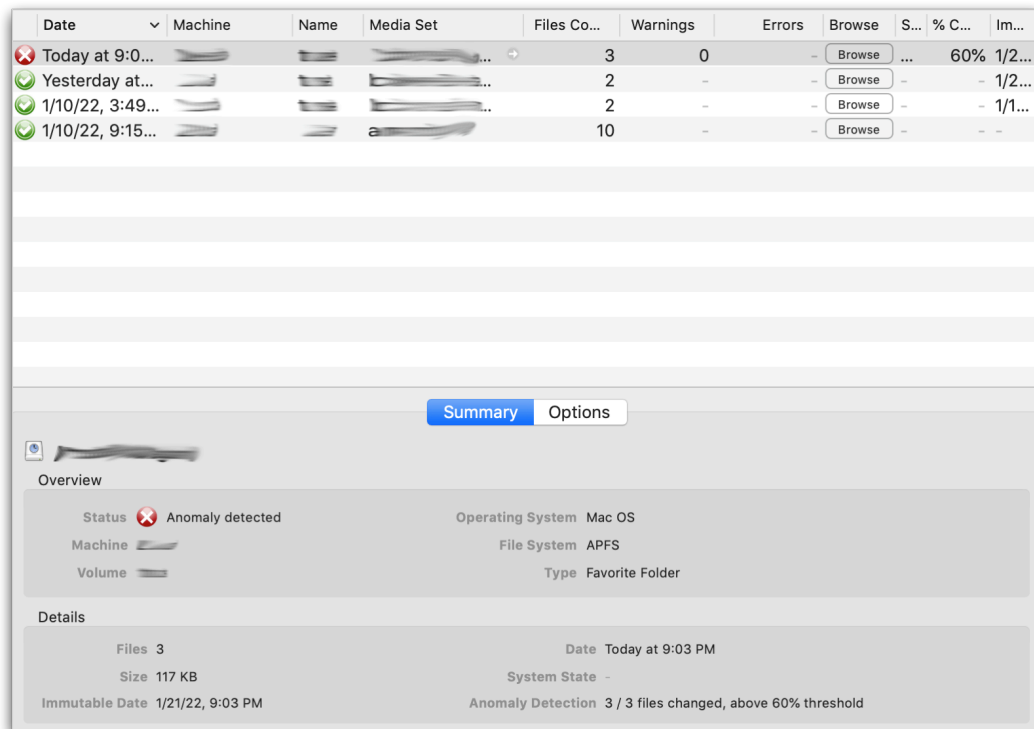
Email



Retrospect Management Console



Retrospect Backup for Windows – Backup Report



Retrospect Backup for Mac – Backup Report

You can also integrate Anomaly Detection with third-party notifications services like Slack using Retrospect's Script Hooks and the "AnomalyAlert" event. You can even customize the backup to stop when it detects an anomaly. See [Script Hooks](#) for more information.

Retrospect Cloud Storage

Overview

With Retrospect Backup, businesses around the world can now protect their critical infrastructure on Retrospect Cloud Storage, with complete support for immutable backups and anomaly detection, as well as on-premise with Retrospect's deep support for NAS devices and tape libraries.

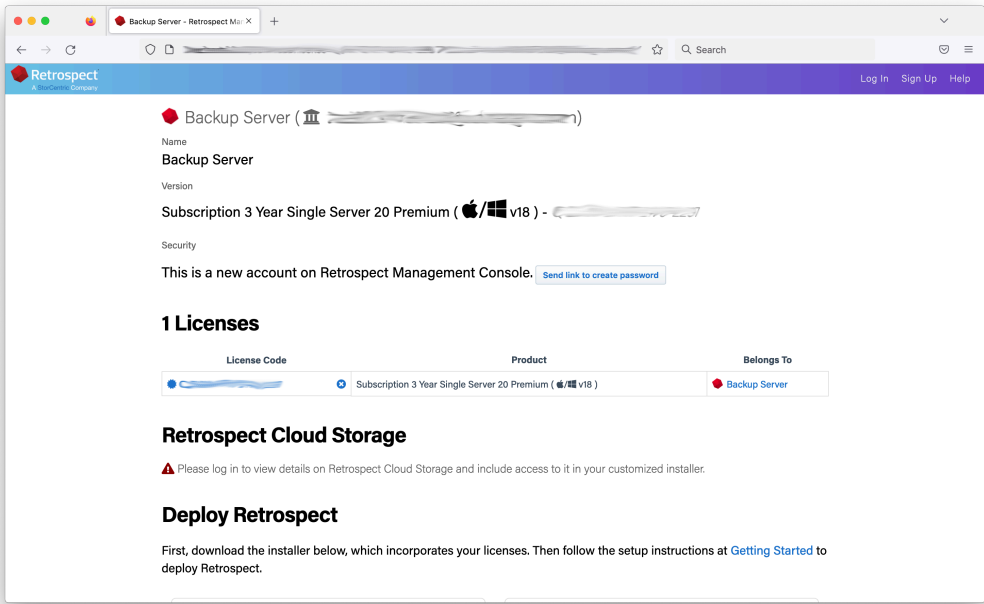
Retrospect Cloud Storage is built on Wasabi Technologies' Hot Cloud Storage, providing lightning-fast object storage. Retrospect Cloud Storage leverages that foundation to provide advanced data protection features like immutable backups. With Retrospect's AES-256 at-rest encryption, sensitive data can be backed up to Retrospect Cloud Storage but guaranteed to remain private from the underlying infrastructure provider, including Retrospect and Wasabi Technologies. Using Retrospect Cloud Storage and the multi-homed backups with the 3-2-1 backup rule, businesses are fully protected and encrypted from ransomware attacks with on-premise and cloud backups.

Tiers

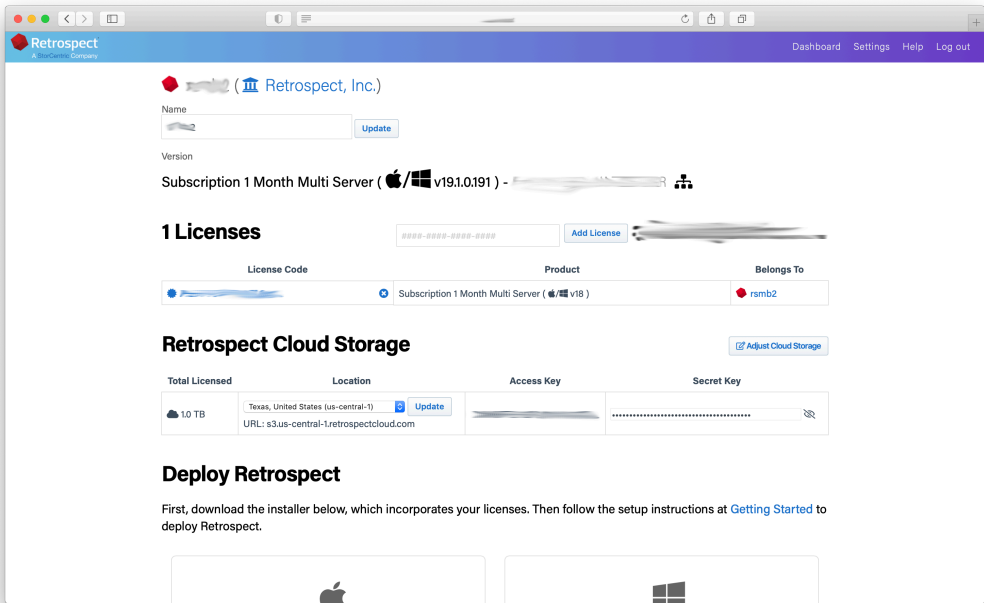
Retrospect Cloud Storage is available as a subscription license, compatible with both perpetual and subscription licenses. It's available as tiers of 1TB, 5TB, and 10TB. Purchase through Retrospect.com for a free 30-day trial.

Setup

If you do not have a Retrospect Management Console account and you click on the link for Retrospect 19 with Retrospect Cloud Storage, you'll see a page like this. We allow you to download the Retrospect application with the license included without signing in, but for security, you must create an account and sign in to access Retrospect Cloud Storage.

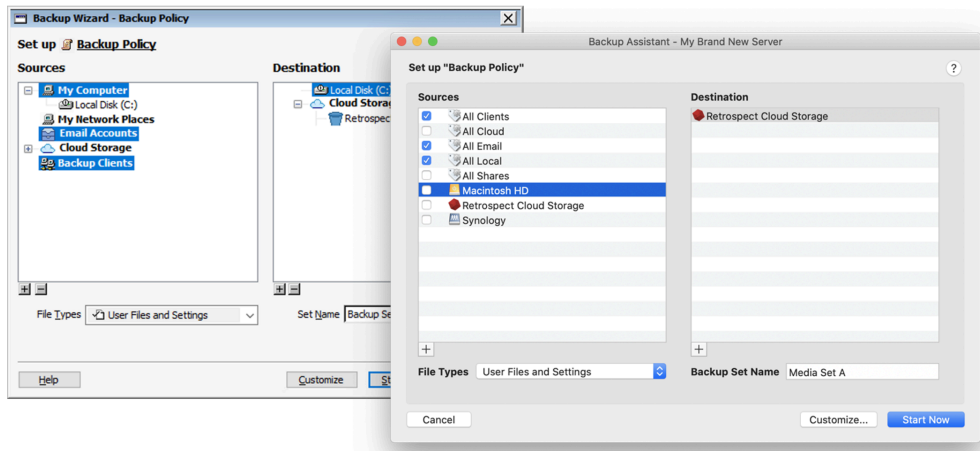


After you sign in, you'll see a page like this.

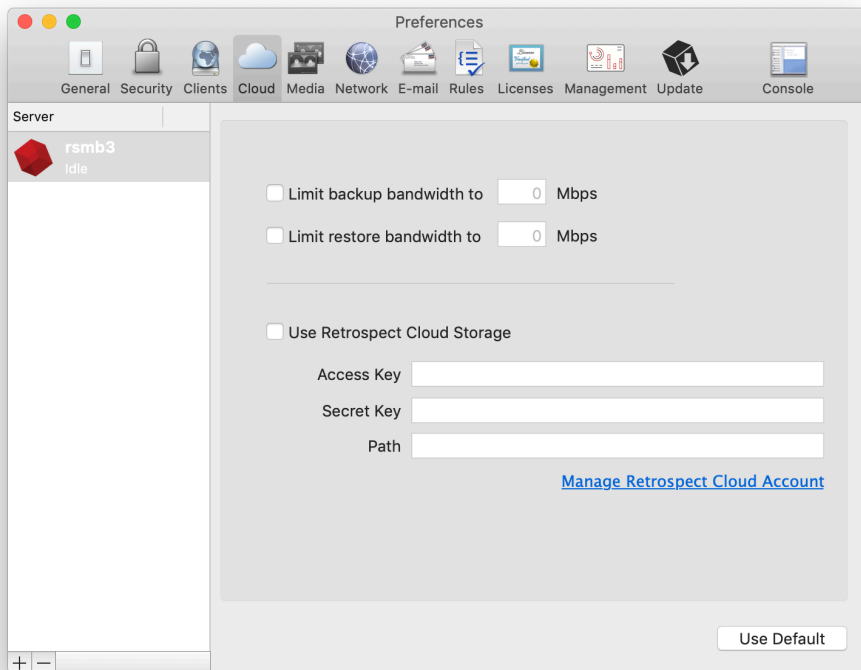


When you download Retrospect from Retrospect Management Console, your license and Retrospect Cloud Storage credentials are included in the personalized configuration file embedded in the download. After you install and launch Retrospect, Retrospect will automatically set up a cloud volume for your Retrospect Cloud Storage account, available in the First Launch wizard.

Retrospect Virtual is fully certified with Retrospect Cloud Storage as well. When you set up a backup set, select "S3-Compatible Storage" and enter the URL, Access Key, and Secret Key from your Retrospect Management Console engine page.



On Windows and Mac, your Retrospect Cloud Storage information is displayed in Preferences > Cloud.



Security Reporting

Security is critical to any business environment, and security reporting helps ensure your business is protected.

Reporting Functionality

Retrospect Backup surfaces the wealth of data it can see into a broad set of reporting improvements to bring security to the forefront.

Retrospect Backup includes detailed backup report for Windows, Mac, Email, Export and the Management Console, ensuring a clear, consistent experience across each product. Email reporting is now available daily and weekly to stay up to date on the status of your backups and emails include the exported report as an attachment.

With the "% Changed" column, administrators can see if there are any volumes that have changed a significant amount, alerting to any significant changes in their data protection, such as a ransomware attack or an incorrect volume backed up.

Let's walk through security reporting with Retrospect Backup:

Backup Report: The "Backup Report" is available under Reports on Windows and Past Backups on Mac. You'll see every source that has been protected or not protected as well as the "% Changed", "Last Successful Backup Date", "Total Files" and many other pieces of data.

Retrospect Management Console: The "Backup Report" is available for your entire environment, across Retrospect Backup engines, using the Management Console under the "Backup Report" tab along the top. It shows a consolidated list of all sources in your environment with the same fields from the backup report on Windows and Mac.

Geo Tracking Endpoints

Tracking assets and ensuring each is properly protected helps businesses see their worldwide asset footprint for their backup environment.

Type	Name	Location	Last Update
User	[Redacted]	[Redacted]	3/4/2021, 11:34:08 AM
User	[Redacted]	[Redacted]	3/8/2021, 12:46:42 PM
User	[Redacted]	[Redacted]	1/4/2021, 10:08:52 AM
User	[Redacted]	[Redacted]	2/9/2021, 3:18:57 AM
User	[Redacted]	[Redacted]	3/16/2021, 4:17:48 PM
User	[Redacted]	[Redacted]	2/26/2021, 10:53:03 AM

The "Geo Tracking" view on Retrospect Management Console is a worldwide map of all users, Retrospect Backup servers, and remote clients, down to the city. This geo tracking ability helps businesses understand exactly where all of their resources are located. If there is a resource somewhere unexpected, it's easy to spot.

Geo Tracking is provided by Retrospect Management Console, using location lookup based on the public IP address of the user, engine, or remote client.

Let's enable "Geo Tracking" for Retrospect Backup:

Sign up for Retrospect Management Console.

Add the "Organization UUID" from Setup to Retrospect Backup under Preferences > Management Console.

Retrospect Backup will contact the Management Console with its current status, including remote clients.

Retrospect Management Console will look up the location of the logged in user, the Retrospect Backup engine, and any remote clients using their respective IP addresses.

Retrospect Management Console displays these locations in a table and as a map under "Geo Tracking".

Cloud Data Protection

Companies use cloud storage for all sorts of data, from website assets to affordable sharing to ingestible data, and Retrospect Backup includes cloud data protection support for cloud storage as a first-class backup volume. Cloud volumes enable businesses to protect their cloud content on-site with an incremental backup or on a different cloud with an automated policy-driven workflows.

Let's walk through protecting an Amazon S3 location. Retrospect also supports Microsoft Azure, Google Cloud, Backblaze B2, Wasabi, MiniIO, and any other S3-compatible certified cloud provider listed on [Cloud Backup](#).

Information for Retrospect

Retrospect needs three pieces of information to access Amazon S3:

Virtual-Host Path – `your_bucket_name.s3.us-east-1.amazonaws.com`

Access Key – Use the Access Key from above.

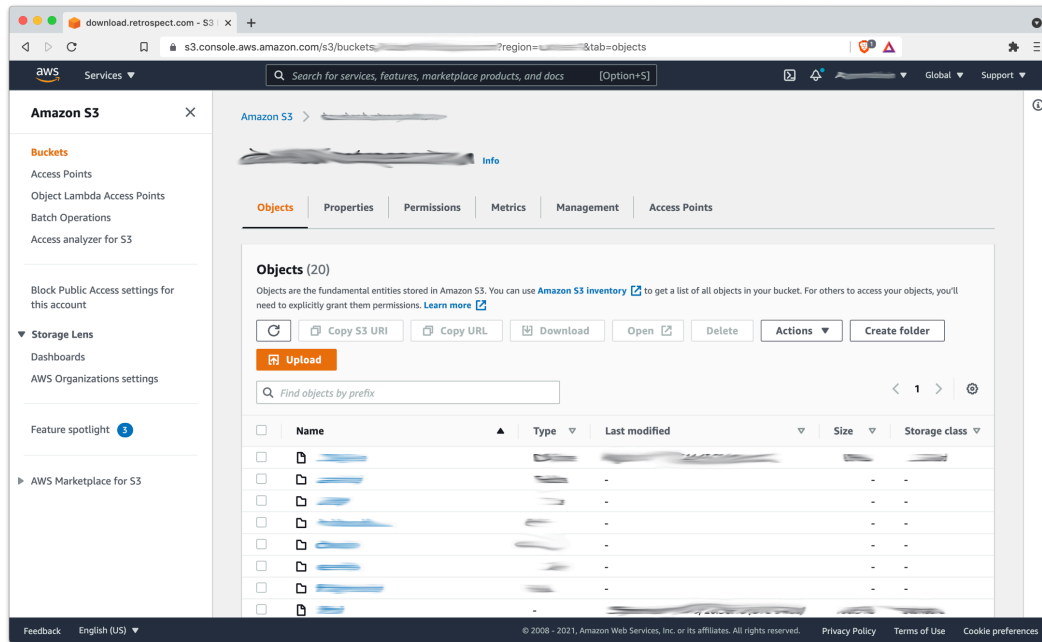
Secret Key – Use the Secret Key from above.

For more information about Amazon S3 and Retrospect, see [How to Set Up an Amazon S3 Account](#).

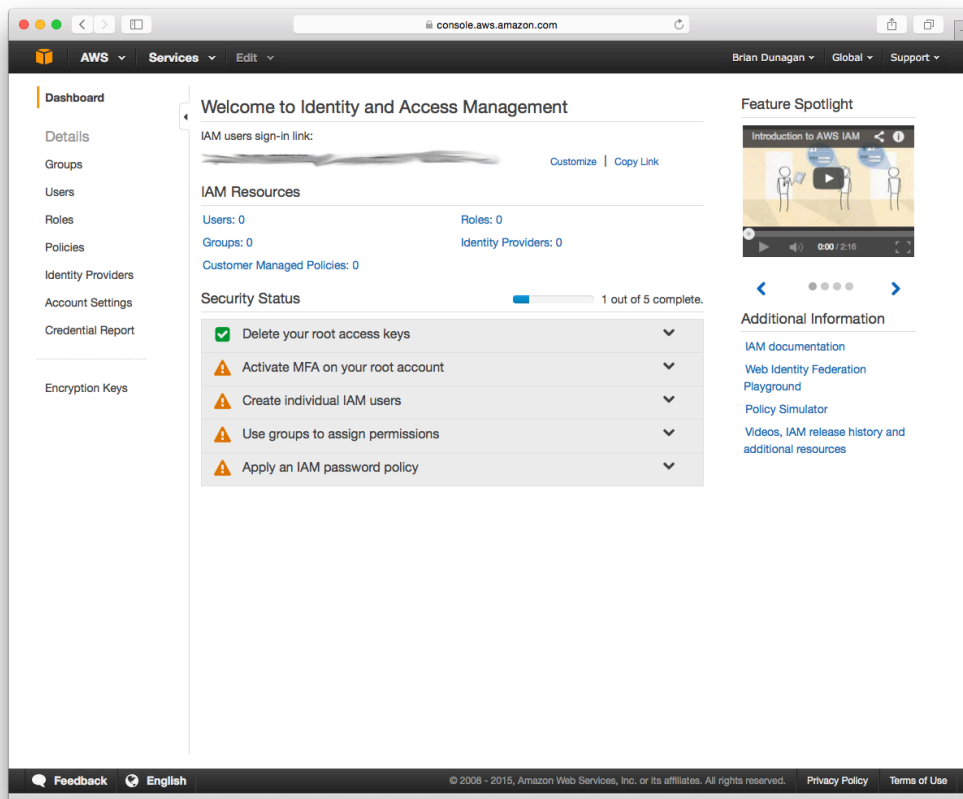
Step-by-Step Guide

Cloud data protection is easy with Retrospect. Let's walk through adding an Amazon S3 volume to Retrospect and then setting up a policy to protect it on-premise.

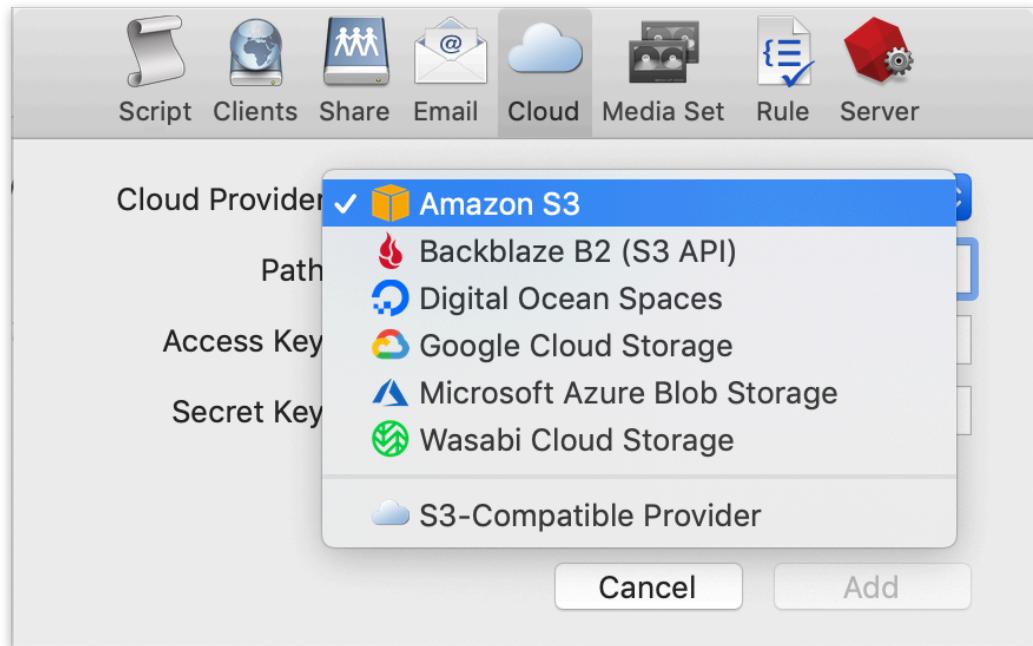
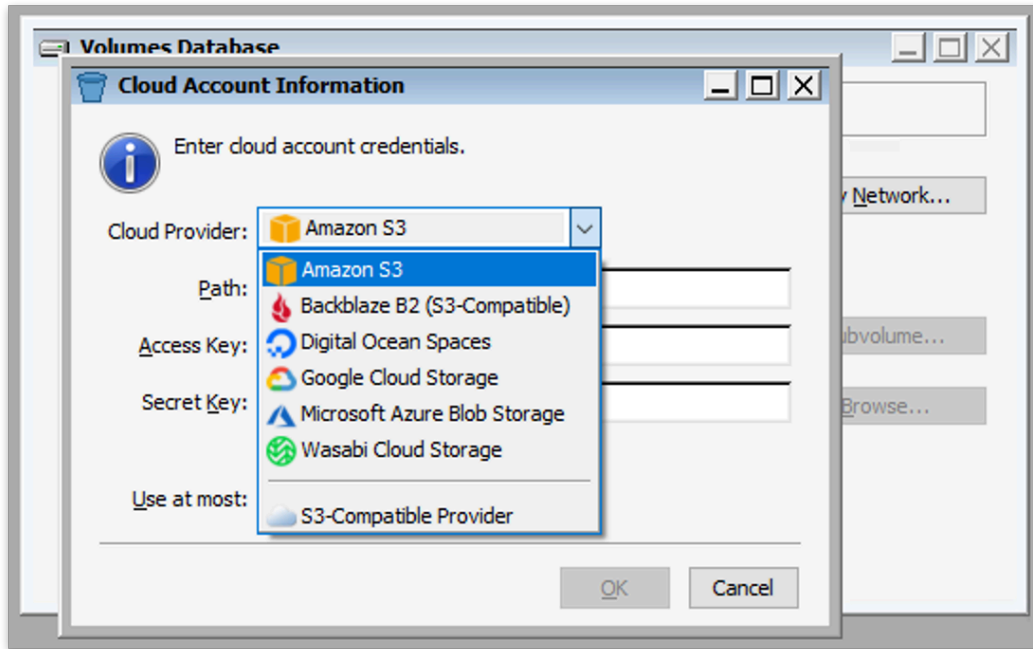
AWS Console: You will need a bucket and path location.



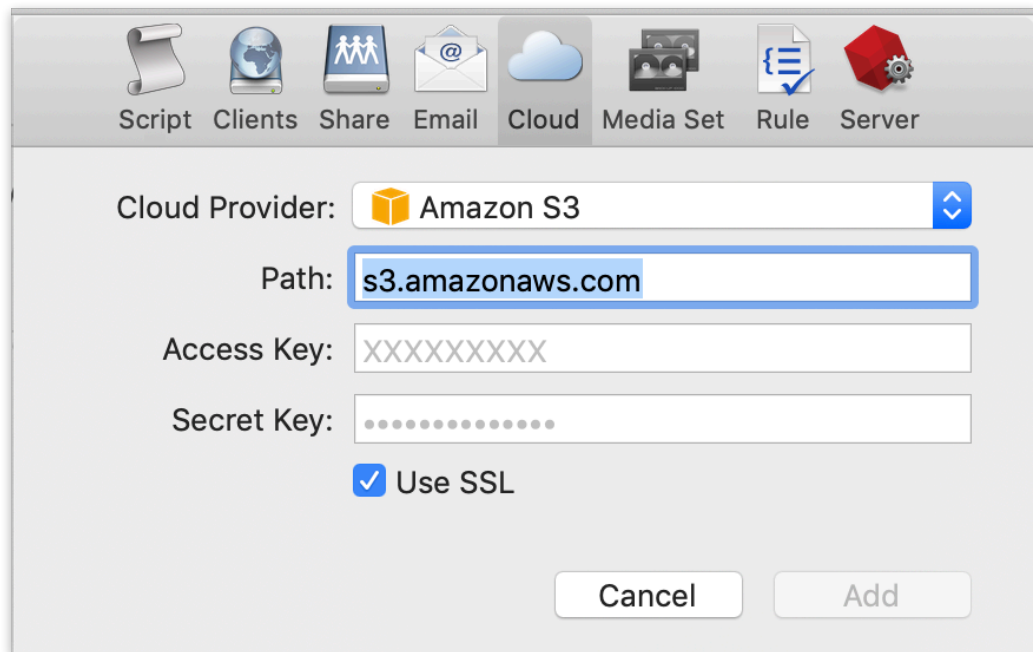
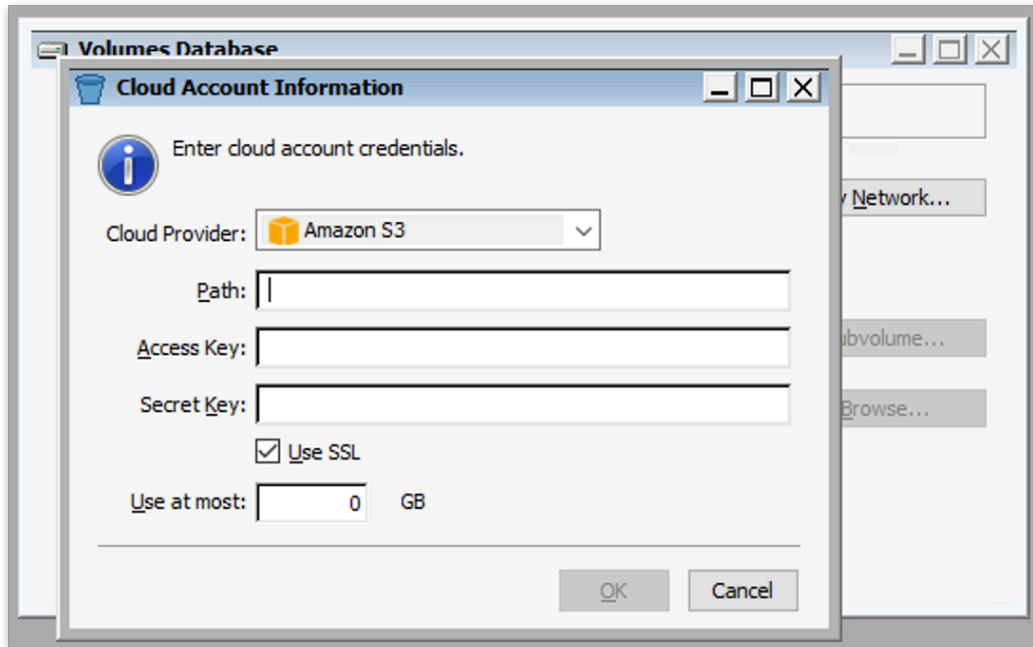
AWS Console: When you created your AWS account, you receive a root Access Key and Secret Key. You can also use IAM to create a user with a specific policy.



In Retrospect, click on "Volumes" (Windows) or "Sources" (Mac).

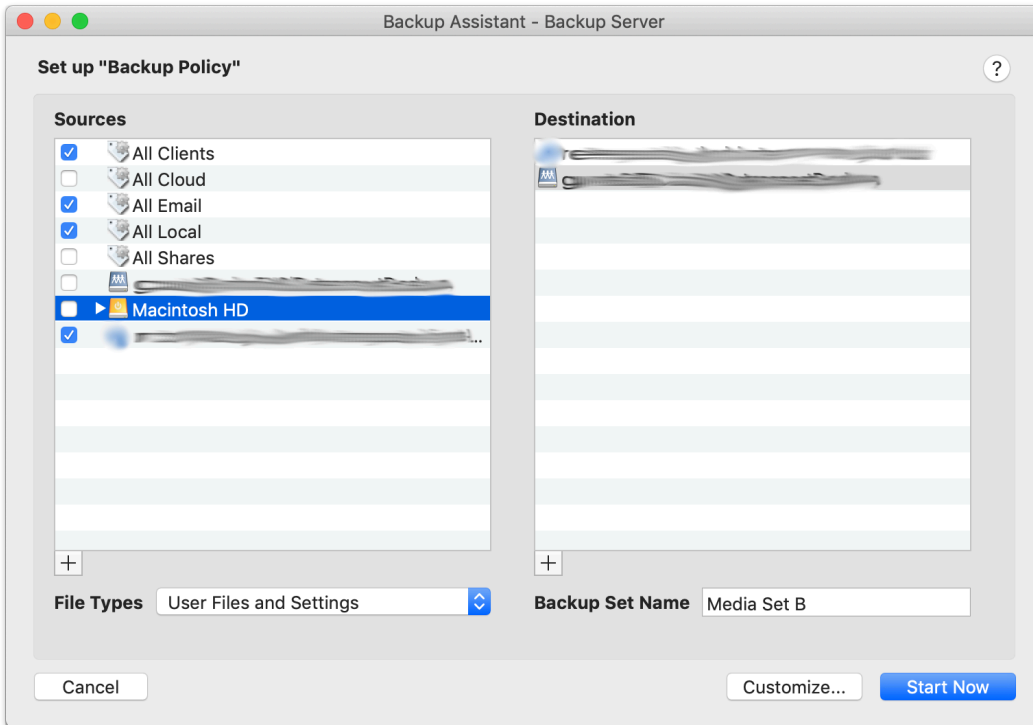
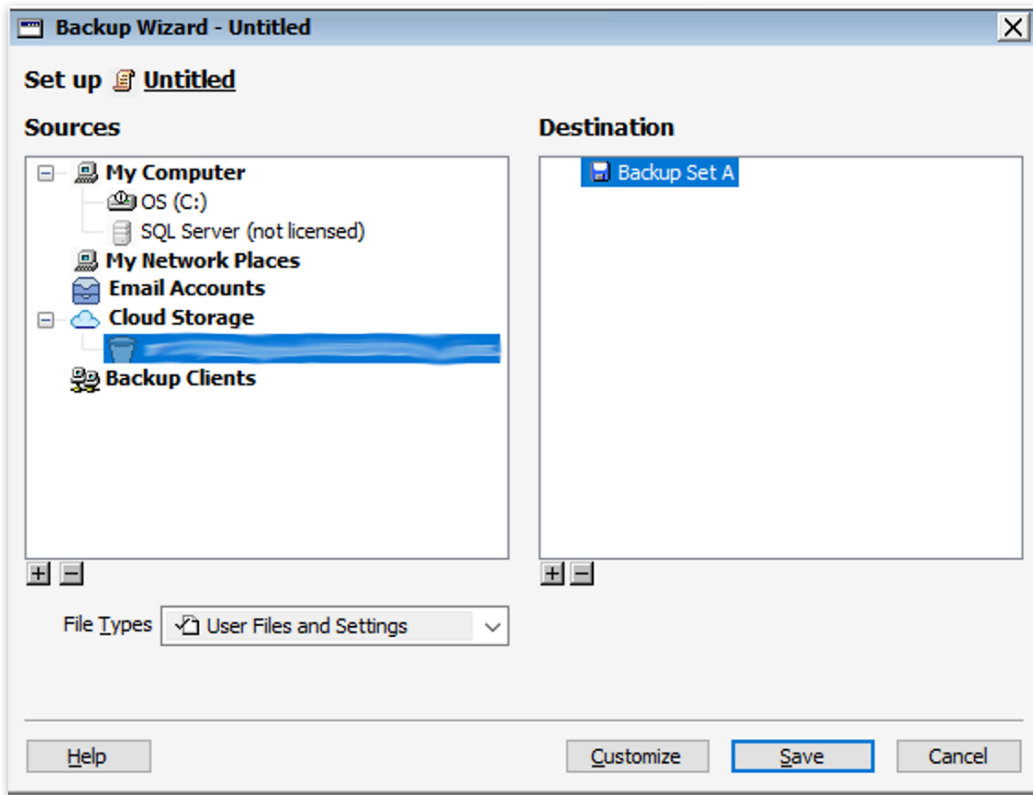


Select "Amazon S3".



Type in your path information and credentials from above and click "OK".

Create a backup script policy for protecting that volume by clicking "Backup Now" (Windows) or "Backup" (Mac).



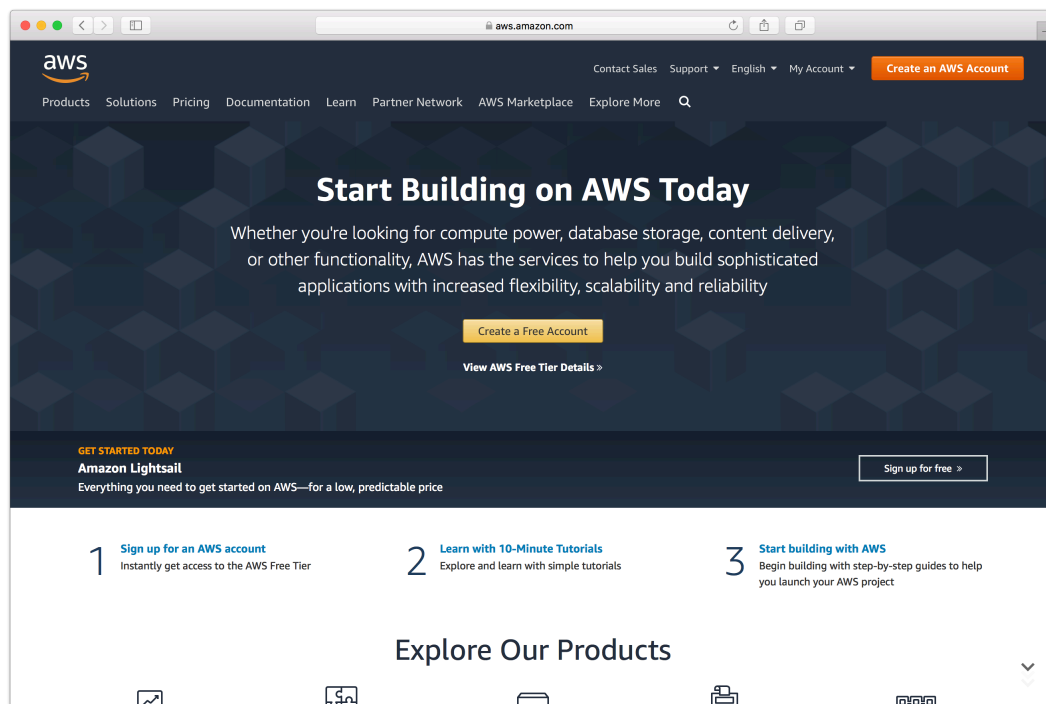
You can now protect your cloud volume using Retrospect, either in another cloud destination or on-premise.

Account Setup Guide

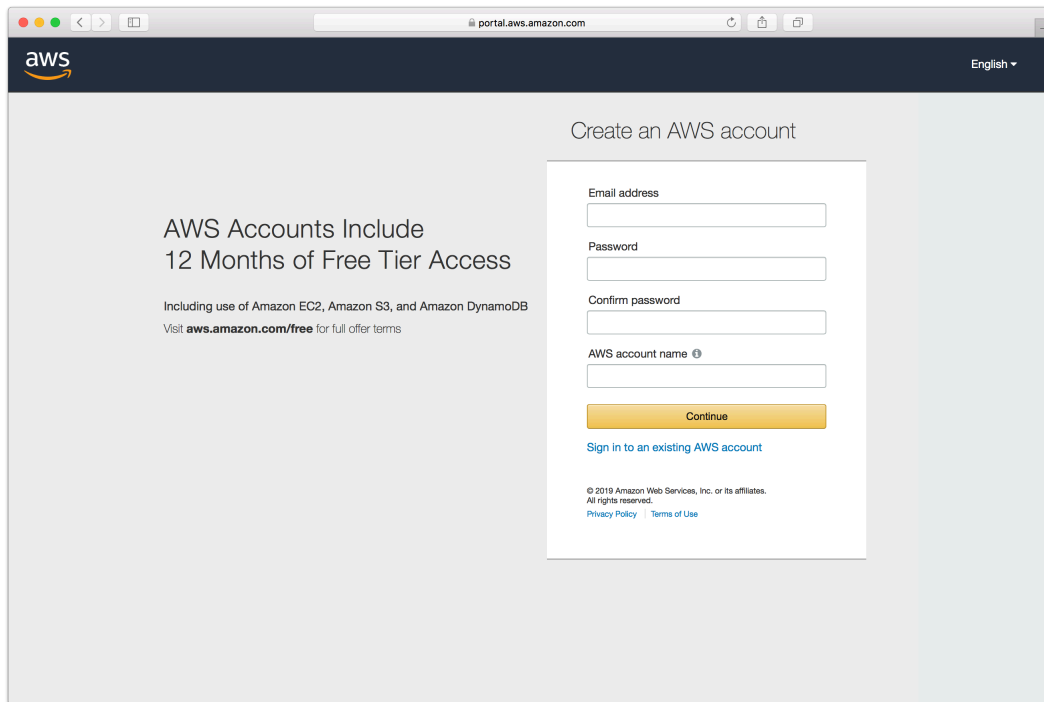
Follow these steps to quickly create a Amazon AWS Account. If you do not already have one, create one for free at [Amazon AWS](#).

See the following video or the steps below to quickly create an Amazon AWS account.

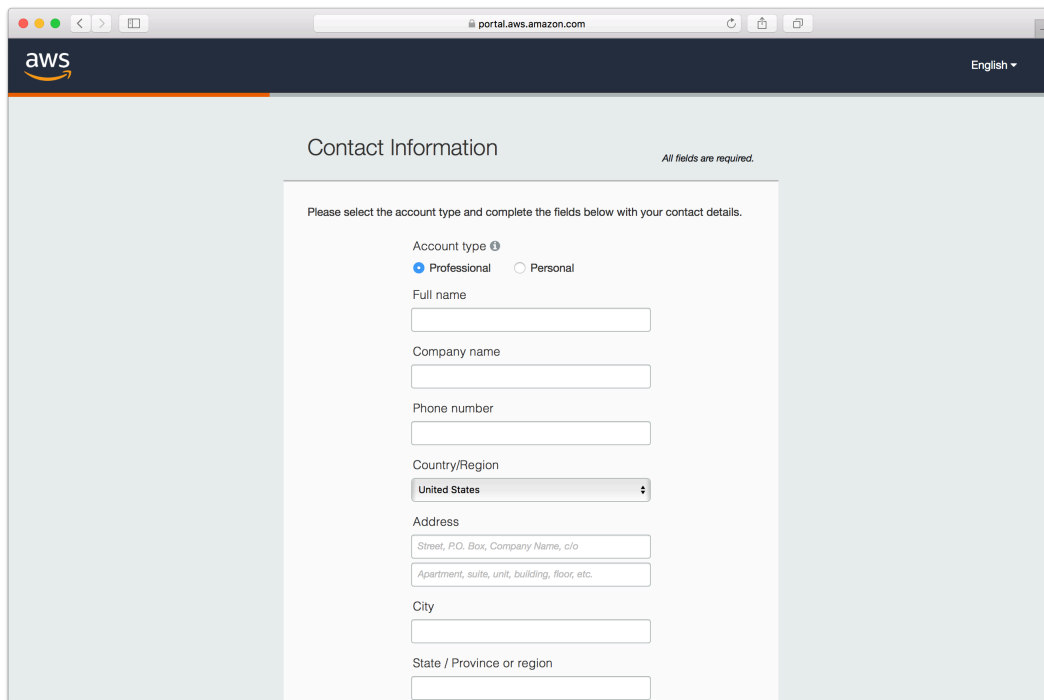
Visit [Amazon AWS](#) to start the account creation process and click "Create an AWS Account".



Fill in an email address and password.



Complete the contact information form.



Complete the payment information form.

The screenshot shows the 'Payment Information' page on the AWS portal. The page title is 'Payment Information'. Below the title, there is a message: 'Please type your payment information so we can verify your identity. We will not charge you unless your usage exceeds the [AWS Free Tier Limits](#). Review [frequently asked questions](#) for more information.' The form contains the following fields and options:

- Credit/Debit card number: A text input field.
- Expiration date: Two dropdown menus, the first showing '08' and the second showing '2019'.
- Cardholder's name: A text input field.
- Billing address: A section with two radio button options:
 - Use my contact address: 1547 Palos Verdes Mall Suite 155, Walnut Creek CA 94597, US.
 - Use a new address.
- Secure Submit: A yellow button.

At the bottom of the form, there is a copyright notice: '© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved.' and links for 'Privacy Policy', 'Terms of Use', and 'Sign Out'.

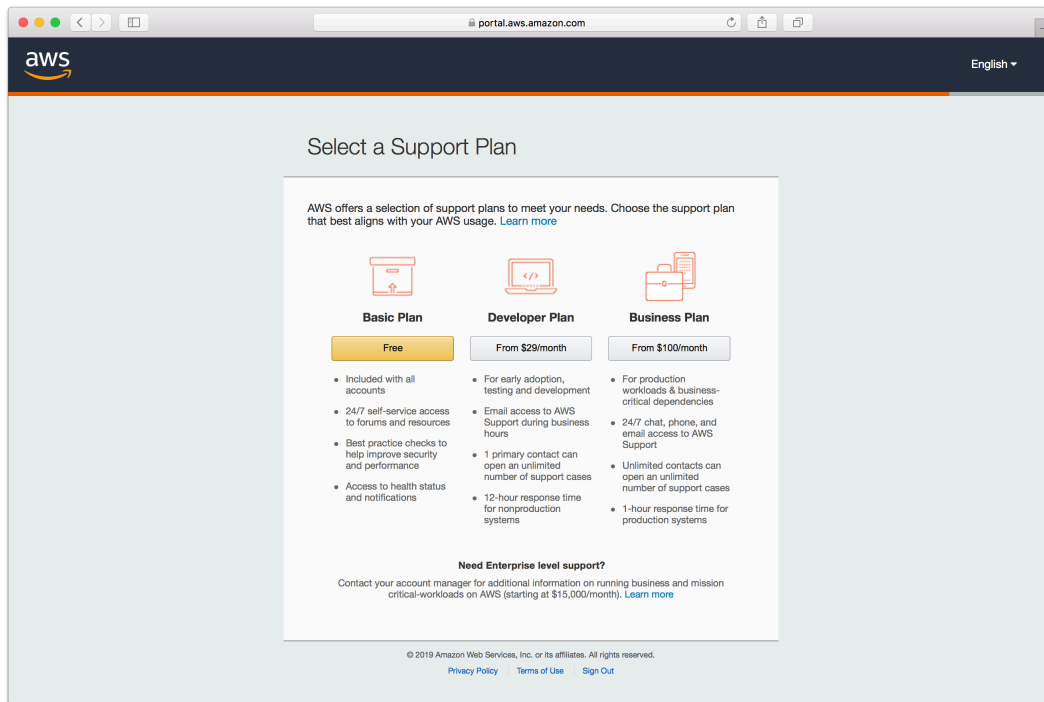
Complete the identity verification.

The screenshot shows the 'Confirm your identity' page on the AWS portal. The page title is 'Confirm your identity'. Below the title, there is a message: 'Before you can use your AWS account, you must verify your phone number. When you continue, the AWS automated system will contact you with a verification code.' The form contains the following fields and options:

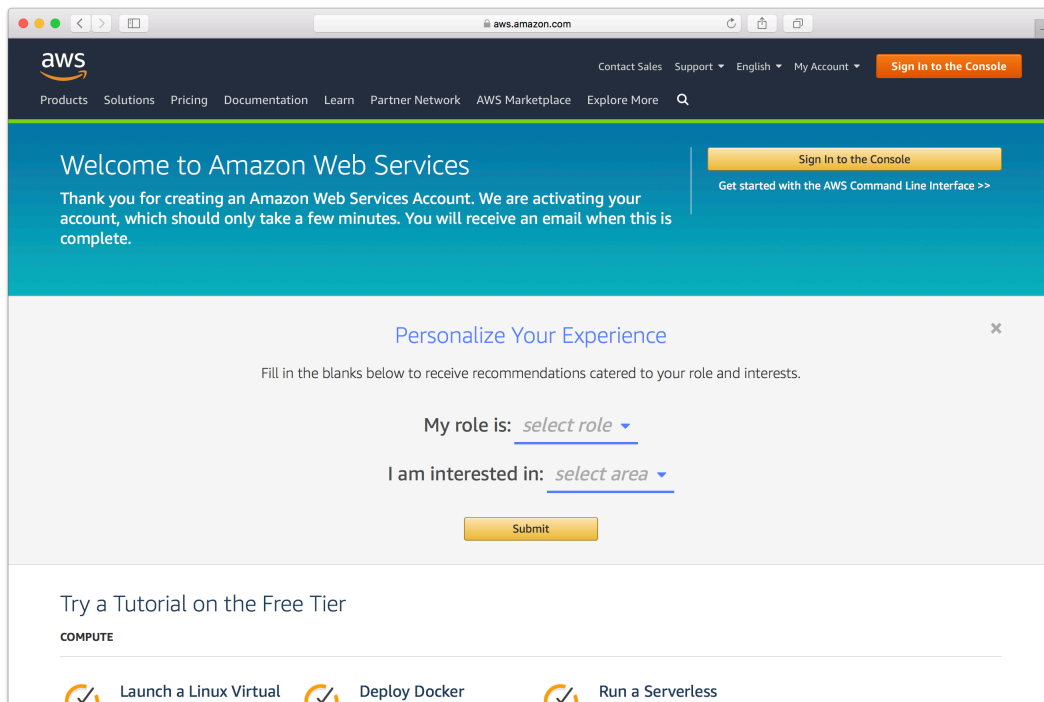
- How should we send you the verification code?: Two radio button options:
 - Text message (SMS)
 - Voice call
- Country or region code: A dropdown menu showing 'United States (+1)'.
- Cell Phone Number: A text input field.
- Security check: A CAPTCHA image showing the characters 'yn3db8' with a speaker icon and a refresh icon. Below the image is a text input field with the placeholder 'Type the characters as shown above'.
- Send SMS: A yellow button.

At the bottom of the form, there is a copyright notice: '© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved.' and links for 'Privacy Policy', 'Terms of Use', and 'Sign Out'.

Select an appropriate Support Plan.



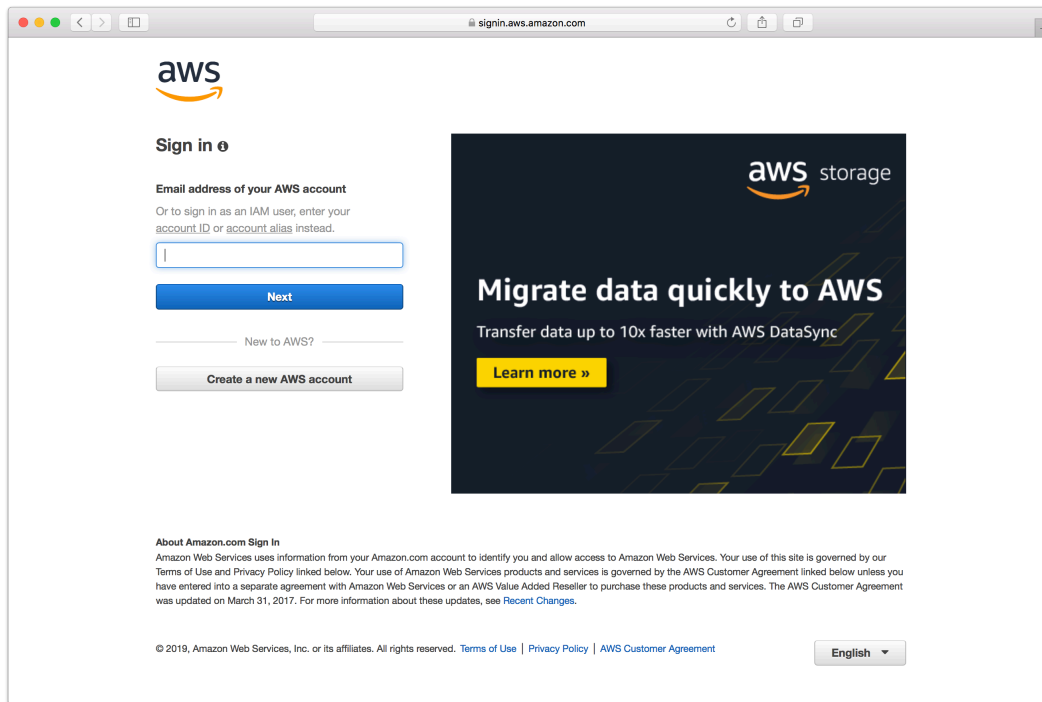
The new account is created.



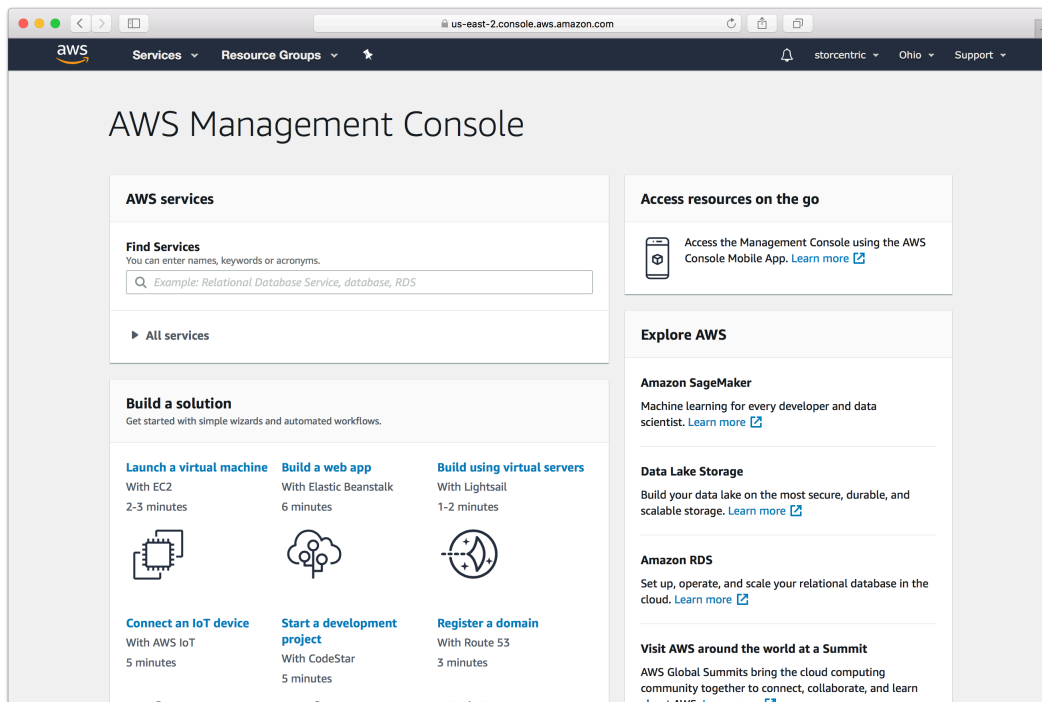
Storage Setup Guide

Now we will create a bucket that Retrospect can use to store backups.

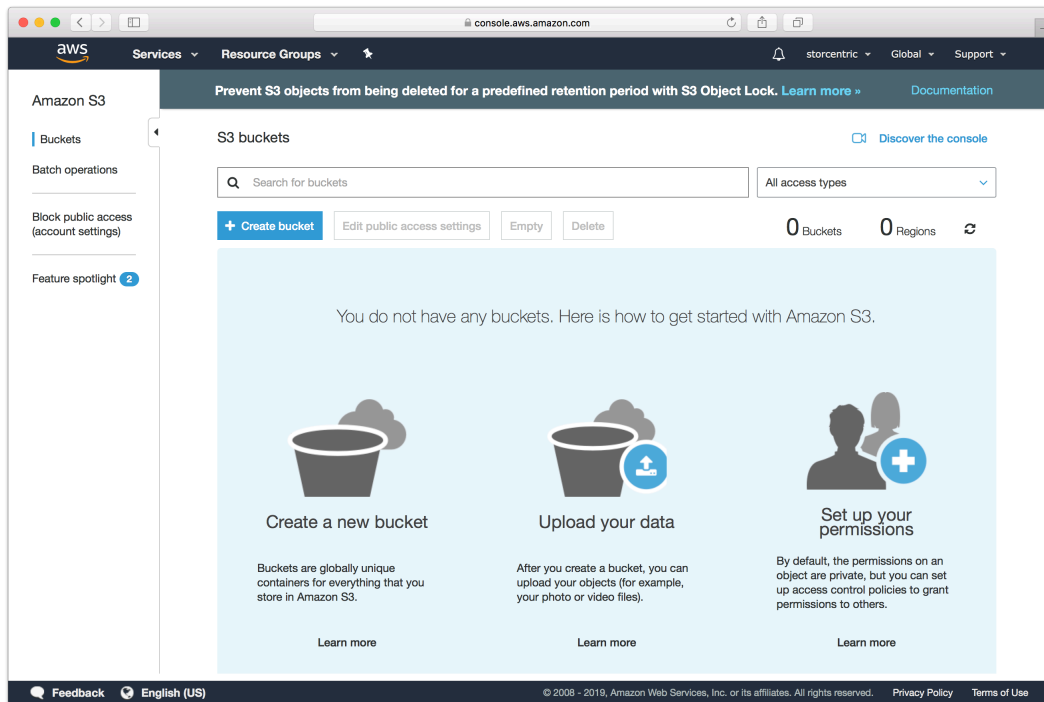
Log into AWS Console.



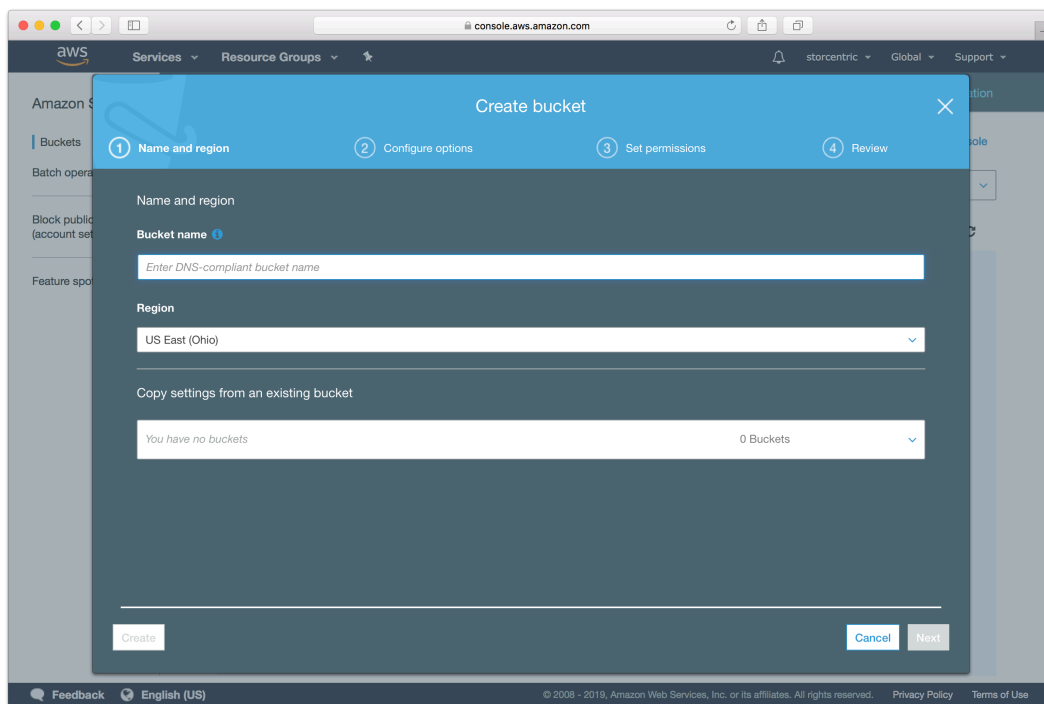
Search for S3 and select.



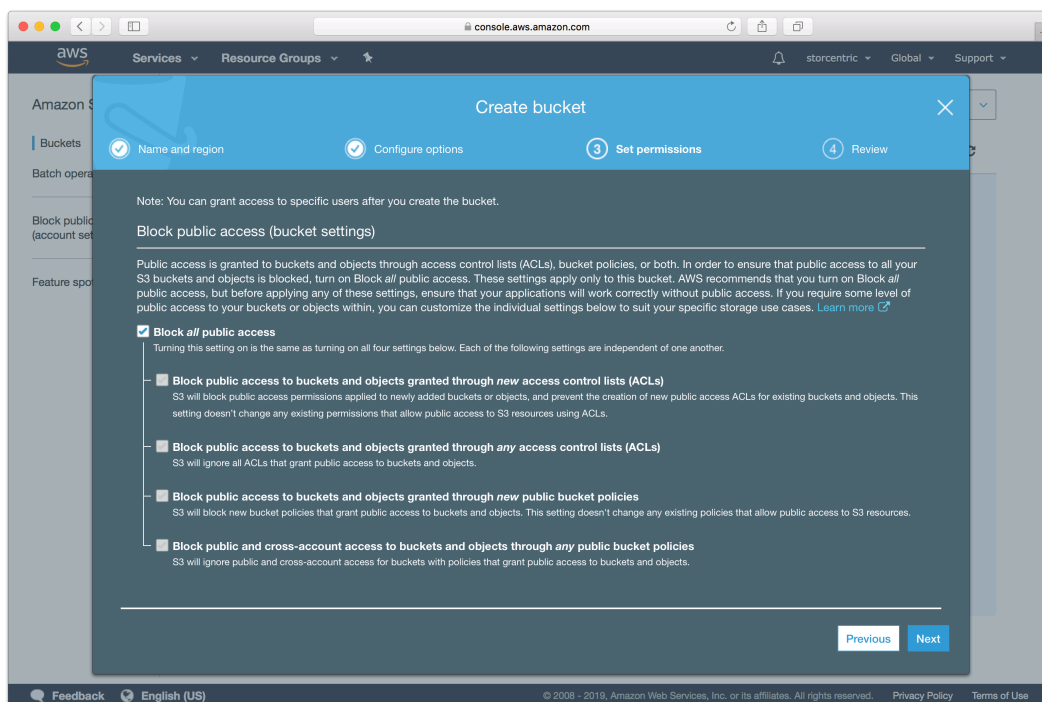
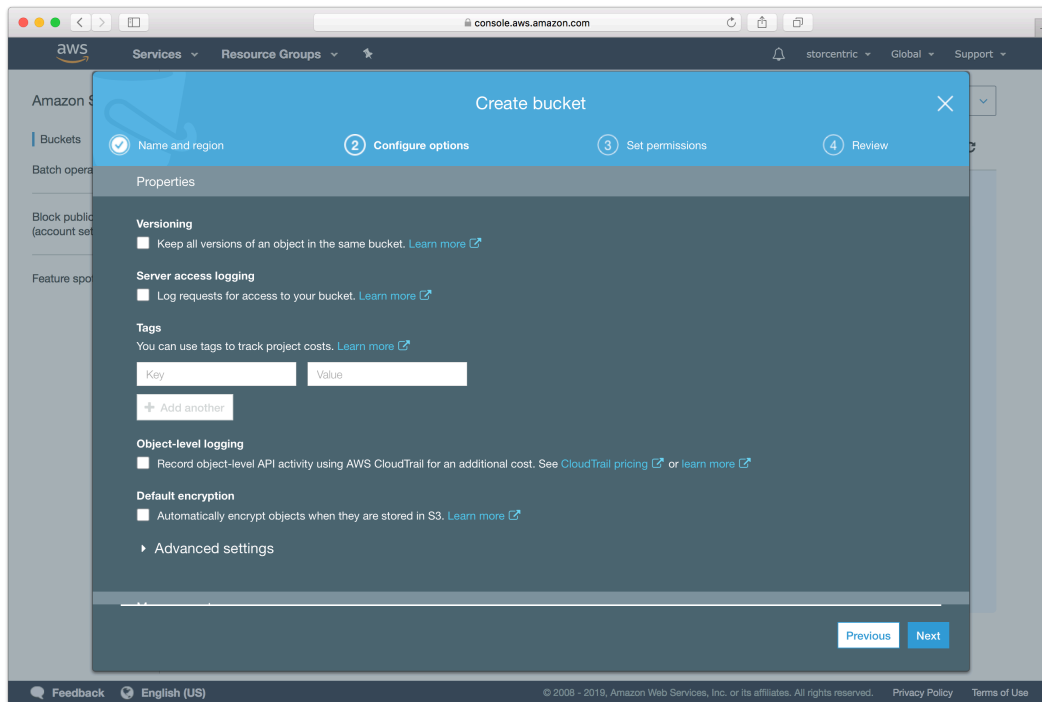
Click "Create Bucket".

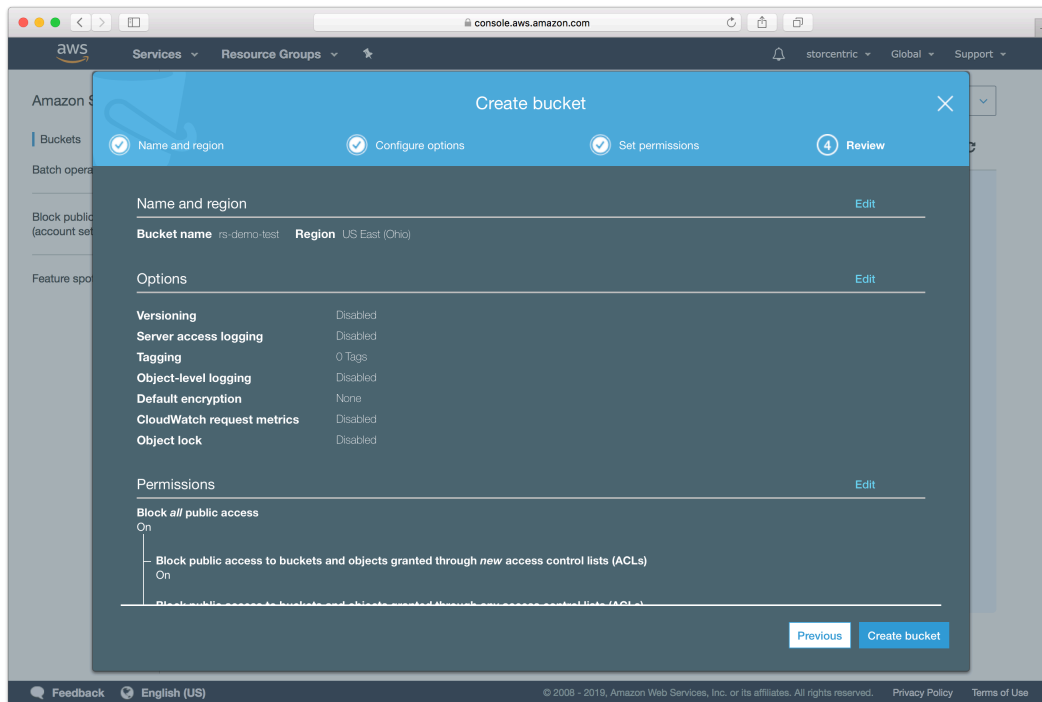


Type in an appropriate name for the bucket. Note that these are globally-unique names.

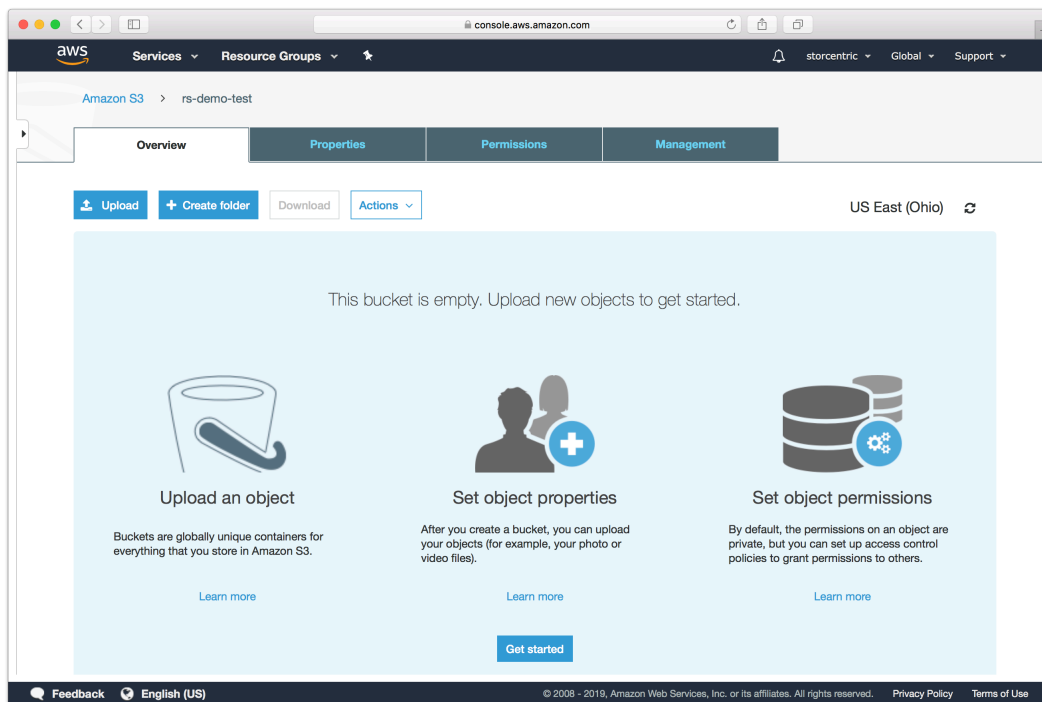


Continue through the rest of the wizard with default options.





Your bucket is now ready. In Retrospect, the "Path" is `s3.amazonaws.com/your_bucket_name`. Next, you need a set of security credentials for Retrospect to use to access it.



Cloud Deployment

Retrospect Backup is a flexible backup solution that you can deploy to the cloud in a virtual machine instance and connect to your on-premise network using a site-to-site connection and a virtual private network.

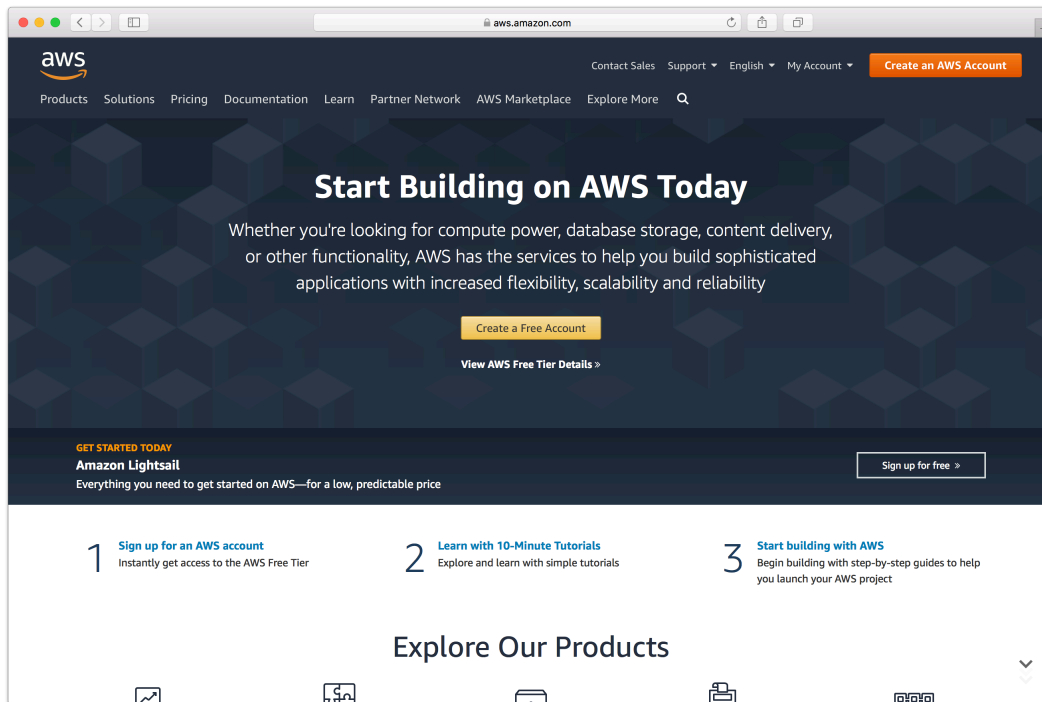
You can deploy Retrospect Backup to Amazon AWS, Microsoft Azure, and Google Cloud. Let's walk through cloud deployment on Amazon EC2.

Account Setup

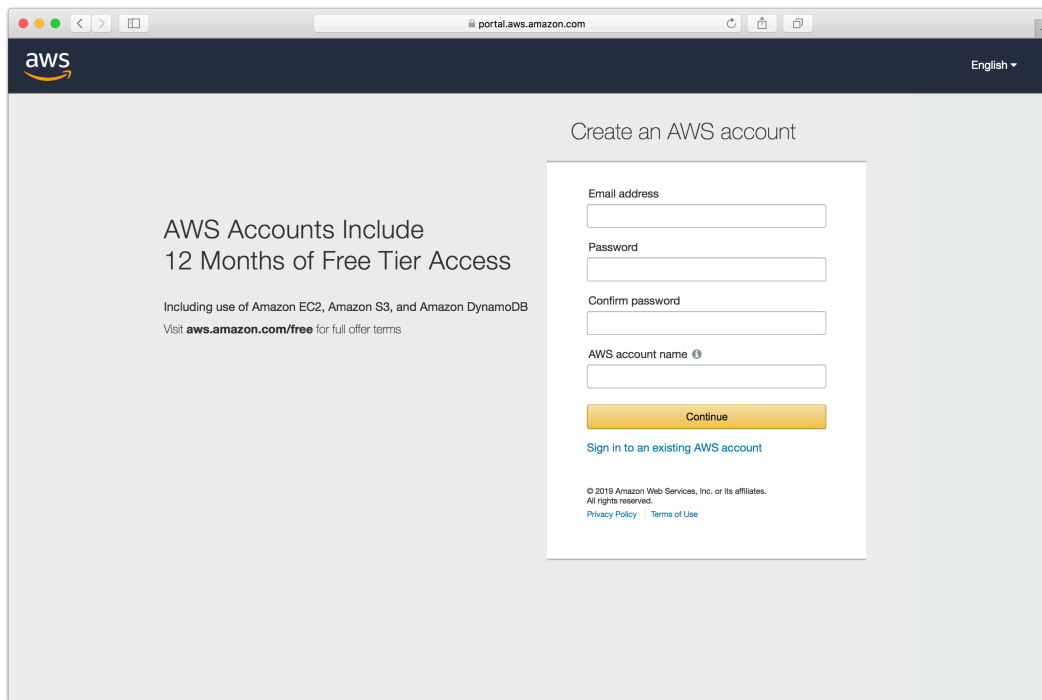
Follow these steps to quickly create a Amazon AWS Account. If you do not already have one, create one for free at [Amazon AWS](#).

See the following video or the steps below to quickly create an Amazon AWS account.

Visit [Amazon AWS](#) to start the account creation process and click "Create an AWS Account".



Fill in an email address and password.



Complete the contact information form.

The screenshot shows a web browser window with the URL `portal.aws.amazon.com`. The page title is "Contact Information" and it includes the note "All fields are required." Below the title, there is a prompt: "Please select the account type and complete the fields below with your contact details." The form contains the following fields and options:

- Account type: Professional, Personal
- Full name:
- Company name:
- Phone number:
- Country/Region:
- Address:
- City:
- State / Province or region:

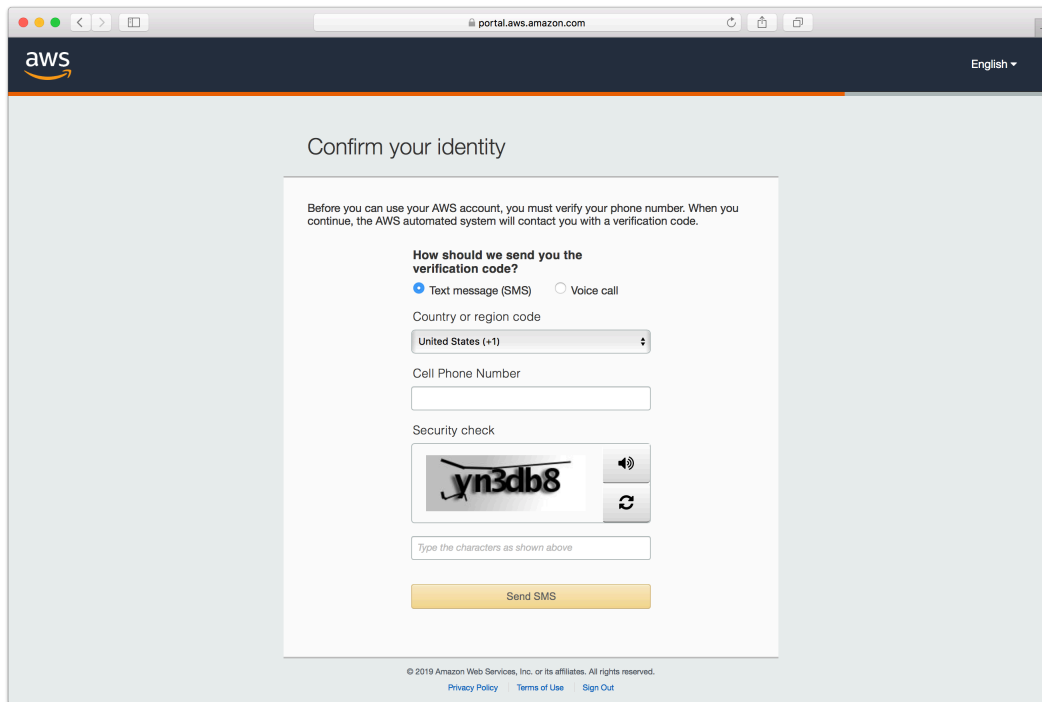
Complete the payment information form.

The screenshot shows a web browser window with the URL `portal.aws.amazon.com`. The page title is "Payment Information" and it includes the note: "Please type your payment information so we can verify your identity. We will not charge you unless your usage exceeds the [AWS Free Tier Limits](#). Review [frequently asked questions](#) for more information." The form contains the following fields and options:

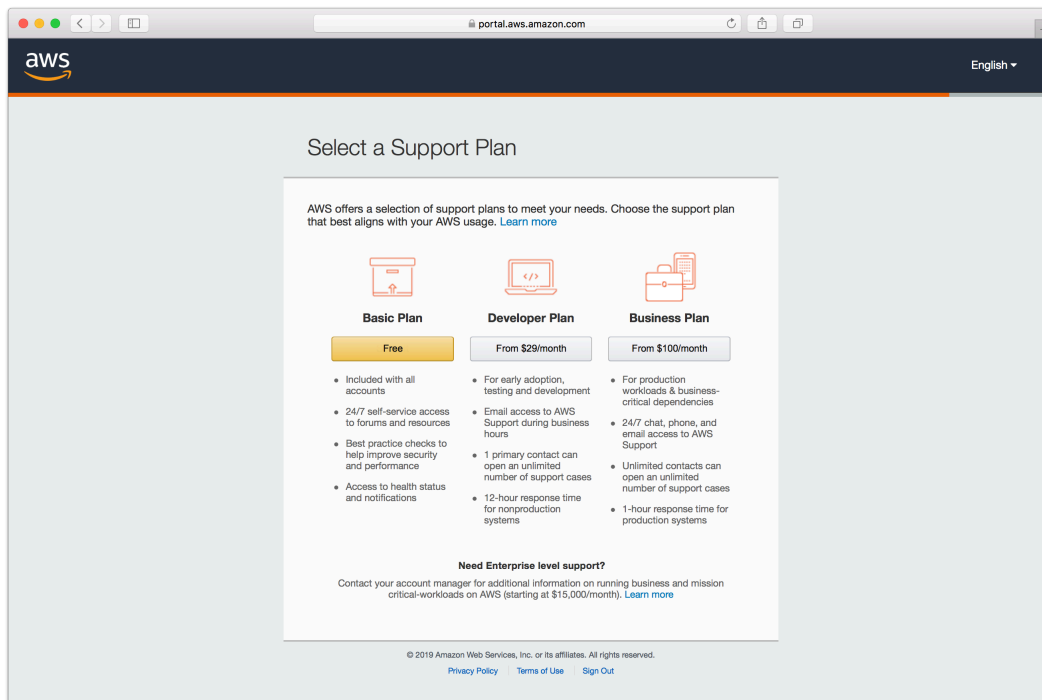
- Credit/Debit card number:
- Expiration date:
- Cardholder's name:
- Billing address: Use my contact address
**1547 Palos Verdes Mall Suite 155
Walnut Creek CA 94597
US**
 Use a new address
- Secure Submit:

At the bottom of the page, there is a copyright notice: "© 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved." and links for [Privacy Policy](#), [Terms of Use](#), and [Sign Out](#).

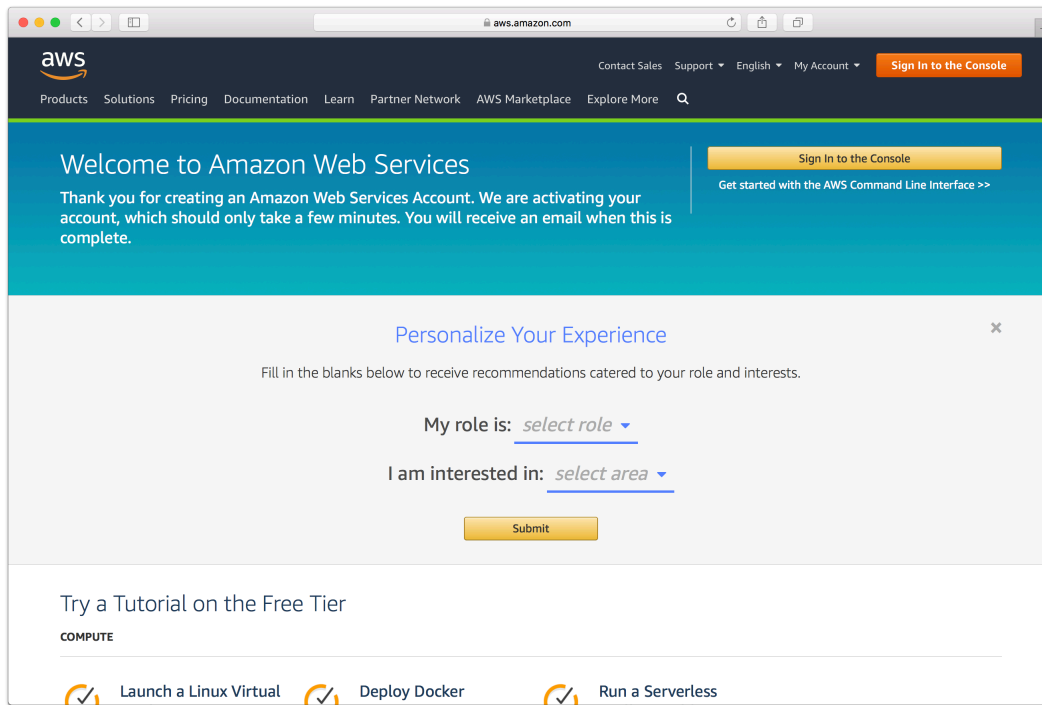
Complete the identity verification.



Select an appropriate Support Plan.



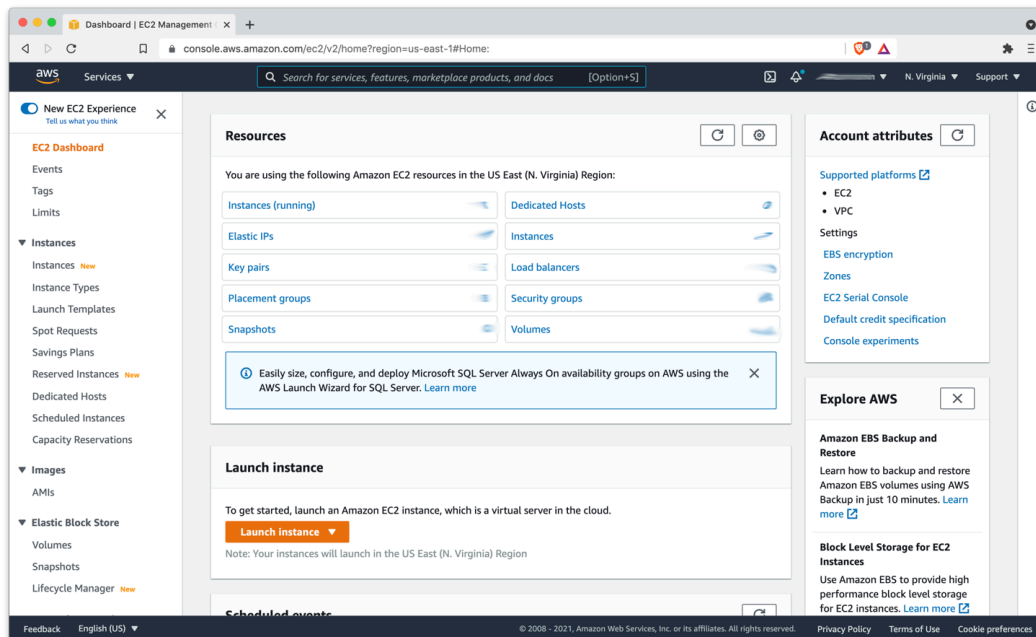
The new account is created.



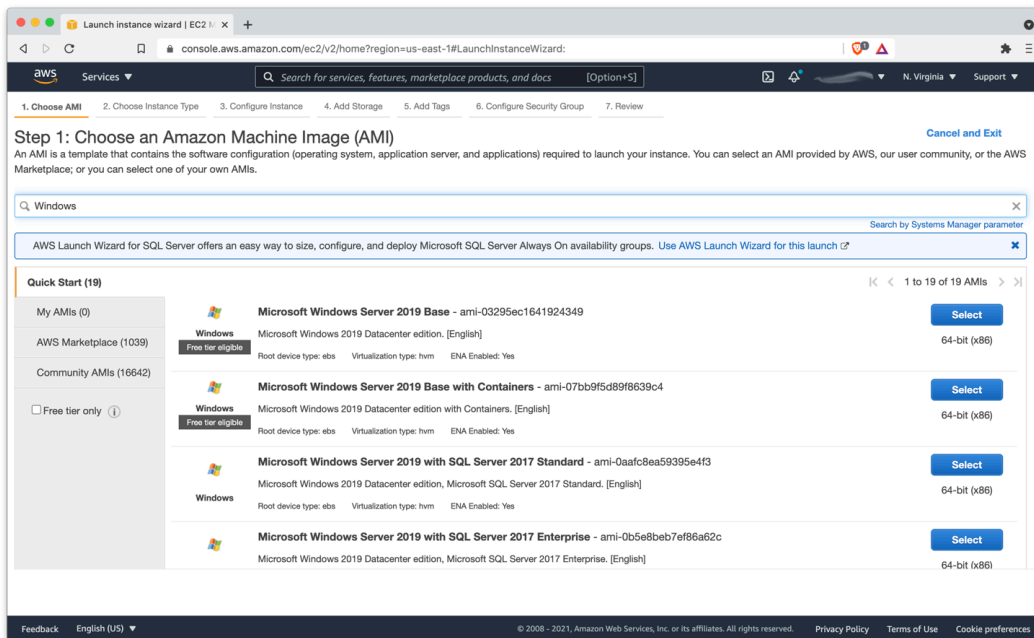
Instance Setup

Retrospect Backup can be installed on any modern Windows OS, both server-level and endpoint-level, including Windows Server 2019. To deploy in AWS EC2, you will need to create a Windows virtual machine and install Retrospect on it.

AWS Console: Visit "EC2" and click "Launch Instance".



AWS Console: Create an appropriate Windows virtual machine.



Instance: After the instance is started, log into it using [Connect to your Windows instance using RDP](#).

Instance: Download Retrospect Backup onto the instance and install the package.

Instance: Run Retrospect Backup and add your license key. You are now ready to use Retrospect. Please see [Retrospect Documentation](#) if you need further assistance.

Remote Backup

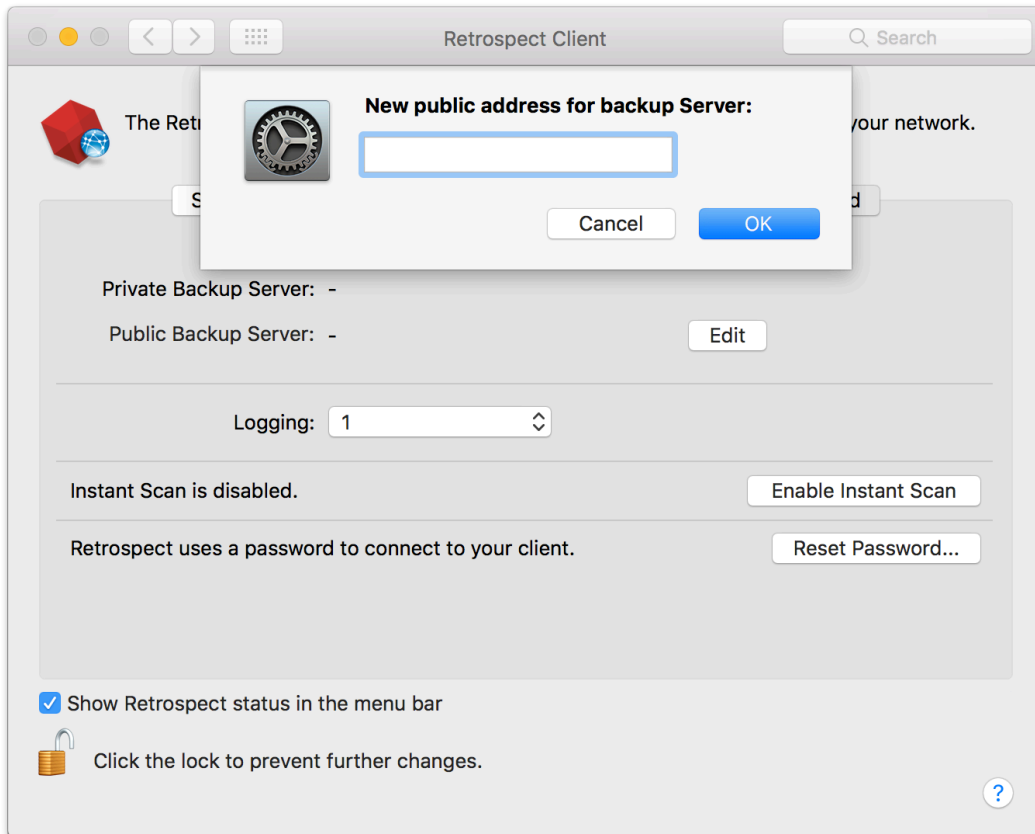
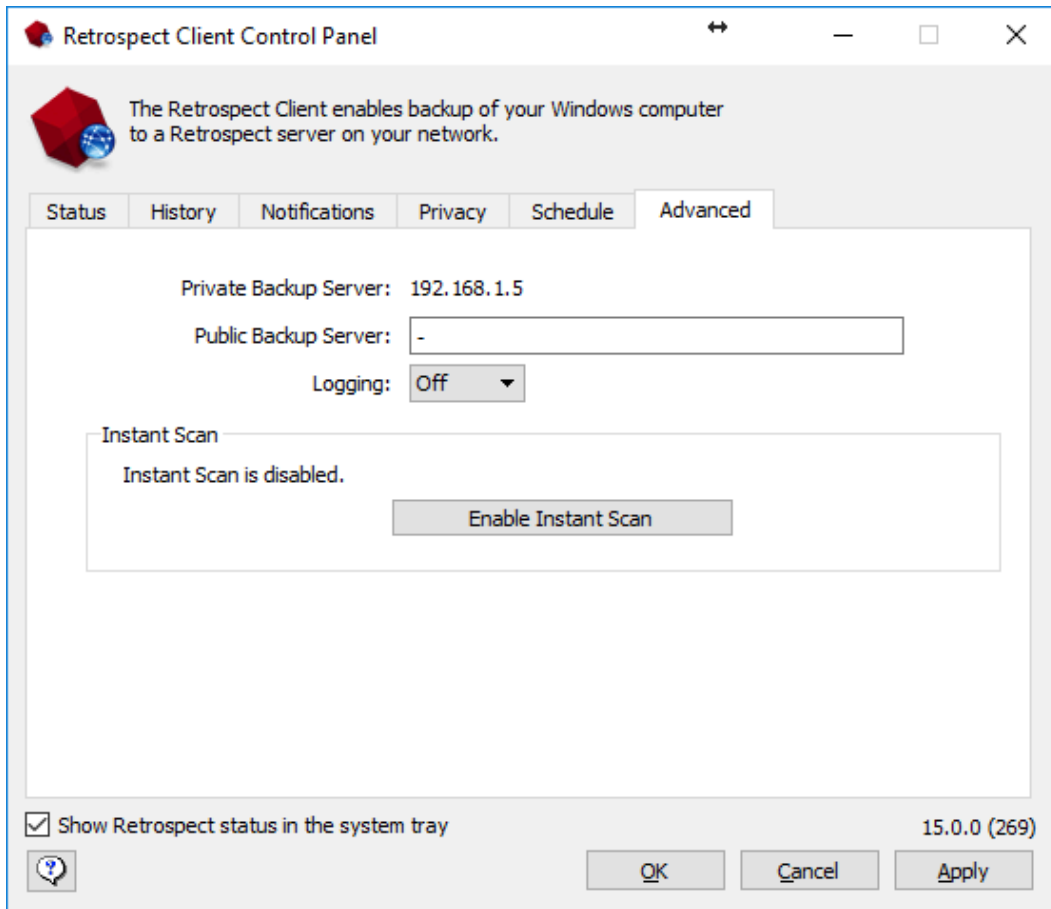
Retrospect supports [Remote Backup](#). This feature allows Retrospect to back up clients from anywhere in the world, regardless of NATs or firewalls. You can set up Retrospect to protect your servers and endpoints using this while Retrospect is running in your EC2 instance.

Record the public-facing IP address or DNS name of the server where Retrospect is running.

Create a public/private key in Retrospect to distribute with your Retrospect Client for authentication.

Download the Retrospect Client onto the server or endpoint that you wish to protect with the public key included.

Open Retrospect Client preferences.



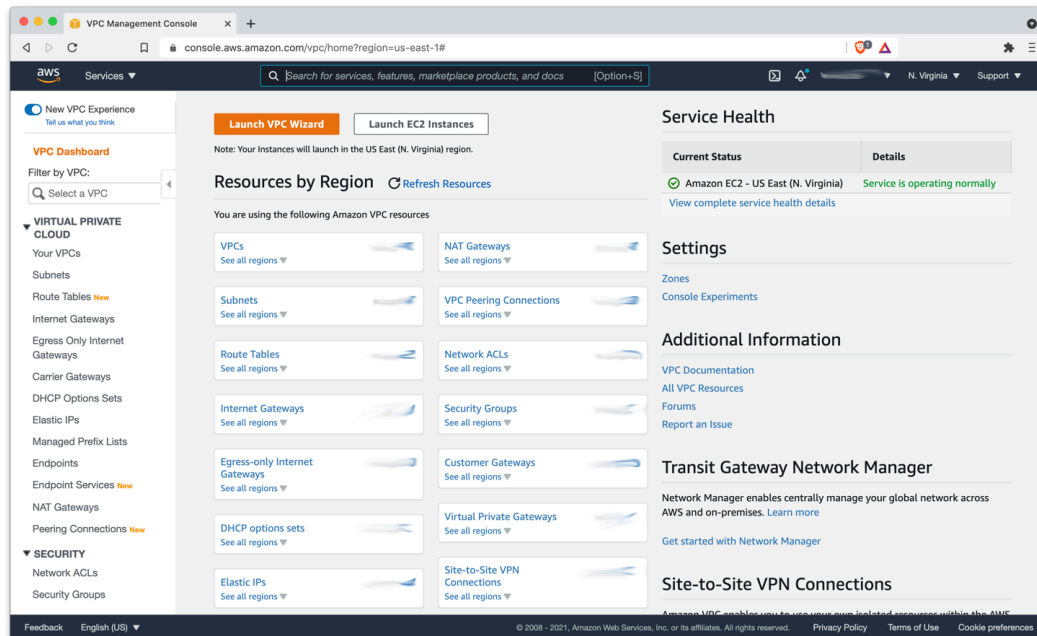
You will need to ensure port 497 and port 22024 are open on the server where Retrospect is running.

Create a ProactiveAI script with "Remote Backup Clients" item selected.

For more details, see [How to Set Up Remote Backup](#).

Virtual Private Cloud (VPC)

AWS provides Virtual Private Clouds (VPC) for creating a virtual private network in their cloud. You can use this to connect multiple VM instances, and you can also use this service to extend your on-premise network with a site-to-site connection. Follow [AWS's What is AWS Site-to-Site VPN?](#)



Use AWS VPC to set up the appropriate virtual network for your business, including a site-to-site connection if it's needed.

Note that multicast traffic is **not supported by AWS VPC**, so you will not be able to auto-discover clients with that method. You will need to manually add IP addresses.

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.

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 “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).

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 under "Catalog and Configuration Backups." In the same chapter, you can find instructions for rebuilding Catalogs, under "Rebuilding a Media Set."

Workflow for macOS El Capitan and Higher

For disaster recovery on El Capitan and higher, you will need to use Retrospect Backup v17.0.1 or higher. It works with macOS System Integrity Protection, which is on Catalina (10.15) back through El Capitan (10.11). The steps differ from past versions of macOS because of this. Before, Retrospect could perform a bare-metal disaster recovery which did not need an underlying OS already installed. However, with System Integrity Protection, the best workflow to restore is installing macOS first and then running a live restore on top of it. This process ensures that Retrospect correctly recovers a user's state, even with newer system protection features like Full Disk Access on macOS Catalina.

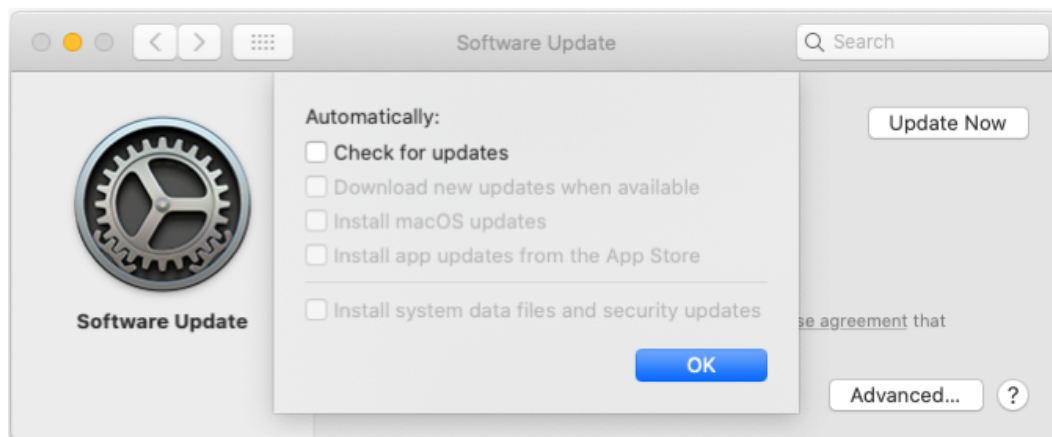
The steps are as follows.

Follow [Apple Support's article](#) to reinstall the macOS version that is in your backup.

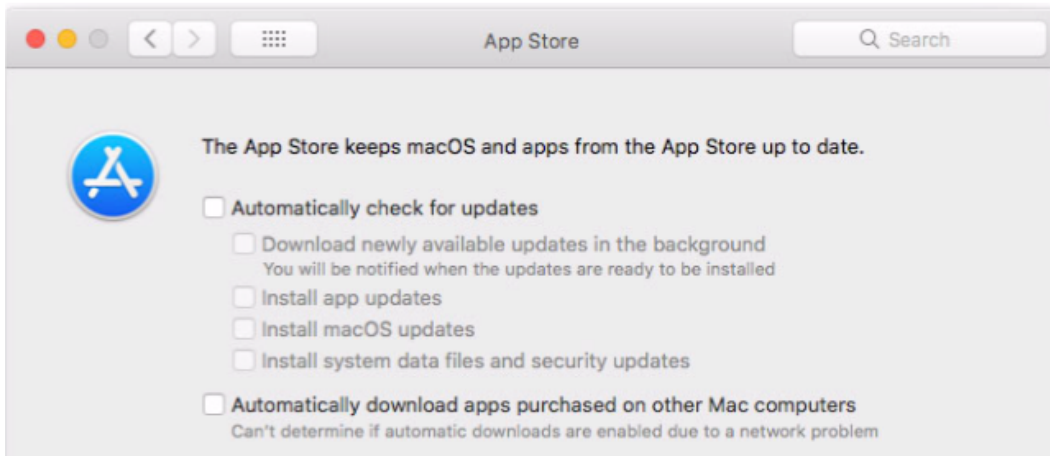
When the newly installed macOS prompts to create a user account, pick an account name that isn't your backup, such as temp_user.

Disable macOS Software Update.

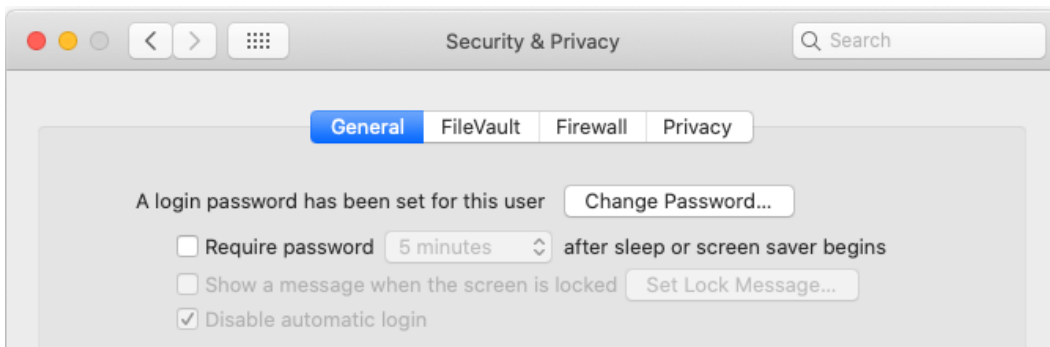
For Mojave or later: System Preferences > Software Update > Advanced > clear the checkbox for "Check for updates".



For an earlier macOS: System Preferences > App Store > clear the checkbox for "Automatically check for updates".



Turn off Screen Lock: System Preferences > Security & Privacy > General > clear the checkbox for "Require password".



Quit all applications.

Install Retrospect or Retrospect Client.

Retrospect needs to be listed under System Preferences > Security & Privacy > Privacy > Full Disk Access. This applies to both a local Retrospect engine and a remote Retrospect Client application. See the [step-by-step guide](#).

Restore the entire macOS volume. During the restore, ignore macOS and application prompts to minimize system changes.

When restore completes, Retrospect would report an expected warning to list folders that are preserved by macOS System Integrity Protection and therefore not restored.

Restart macOS.

User data is restored. On Catalina, recreate user accounts using the exact same names as in the backup and choose "Use existing folder".

Enable macOS Software Update.

Reinstall apps (e.g. Drobo Dashboard) that adds kernel extensions in the "/Library/Extensions" folder.

Workflow for macOS Mavericks and Lower

For macOS Mavericks and lower, there is a different workflow because macOS does not yet include System Integrity Protection.

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

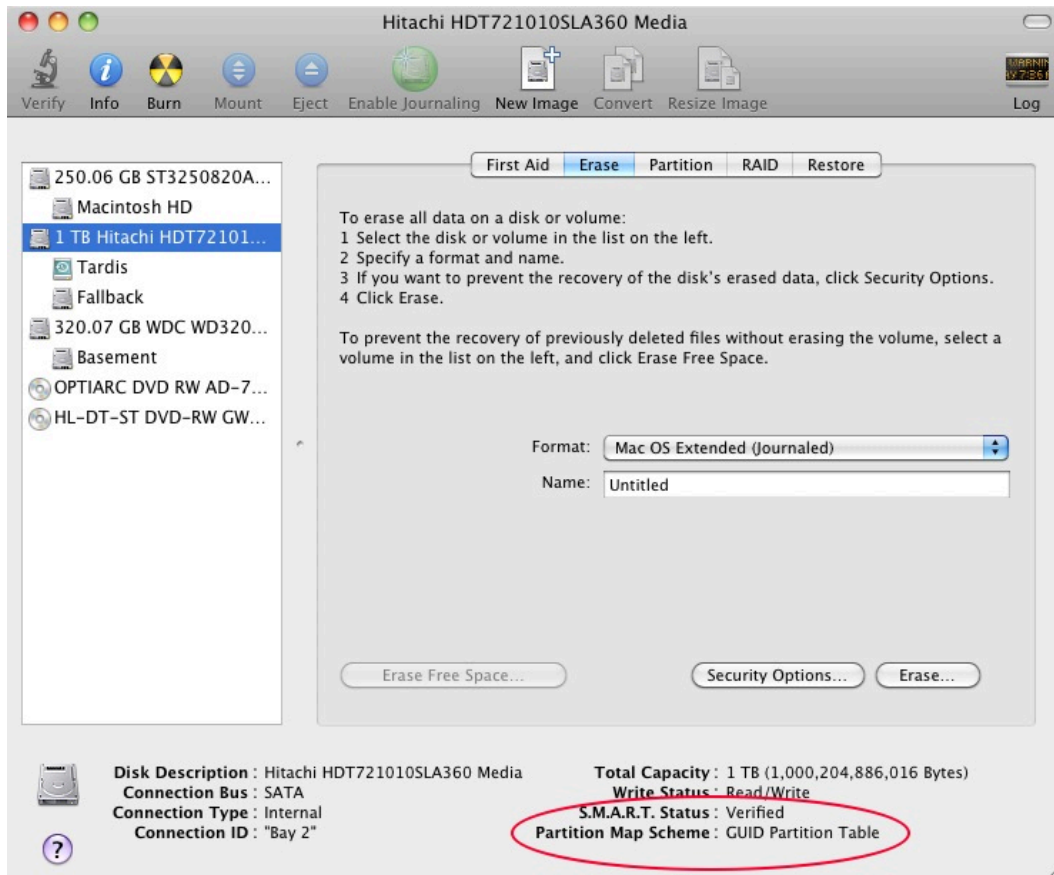
USB or FireWire?

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 partitioning 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.

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:

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.

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.

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

Start the Retrospect console.

(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.

In the Retrospect toolbar, click Restore. The Restore Assistant window appears.

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

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

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.

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

When the restore is complete, eject the Target Disk Mode Mac's disk and start it up normally.

Restoring a Mac using an Emergency Tools disk

In this method of disaster recovery, you will start up the Mac using your previously prepared Emergency Tools hard drive. Follow these steps:

Connect your Emergency Tools hard drive to the Mac you want to restore. Turn on the drive and then start the Mac. Since the 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.

Launch Retrospect and add the catalog file for the Media Set that you want to restore from.

In the Retrospect toolbar, click Restore. The Restore Assistant window appears.

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

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.

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.

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

When the restore is complete, shut down the Mac by choosing Shut Down from the Apple menu.

Disconnect the Emergency Tools disk, then start the restored 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:

If the Mac won't boot, install 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.

On macOS 10.11 and later, follow the steps earlier in this chapter under "Workflow for macOS El Capitan and Higher."

Install the Retrospect Client software on the target Mac.

On the Retrospect server, log in the client to be restored.

In the Retrospect toolbar, click Restore. The Restore Assistant window appears.

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

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.

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.

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

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 Replicated Copy

If you have been using Retrospect's Copy/Replication 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:

Connect the hard drive containing the copy to the Mac you want to boot and restore.

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.

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.

Press the Return key on your keyboard to start the computer from the volume you selected.

Once the startup process is complete, you may use the computer while booted from the backup disk.

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. In this case, you have two options:

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.)

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 steps are to restore specific files and folders onto a functioning remote Windows system. For a disaster recovery scenario, live restores are not recommended in modern Windows OSs, and you should perform a Windows DR bare metal restore. See the Windows User Guide.

Add the Windows client.

In the Retrospect toolbar, click Restore. The Restore Assistant window appears.

Choose "Restore files and folders" then click Continue. The Select Backup pane appears.

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.

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.

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

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."

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.

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.

From the Sources category of the Retrospect console, Remove the old Linux client, then Add the new client.

In the Retrospect toolbar, click Restore. The Restore Assistant window appears.

Choose "Restore an entire source volume or favorite folder to a previous point in time," then click

Continue. The Select Backup pane appears.

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.

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.

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

Restart the client computer.

About Mac OS X's "Recovery HD" partition

The installation process for Mountain Lion and Lion modifies the Mac's startup disk to add a hidden "Recovery HD" partition that can be used to start up the Mac in the event of a problem with the primary startup volume. This partition is not visible in Retrospect or Disk Utility.

Retrospect users should be aware of the following information regarding the Recovery HD partition:

The creation of this partition changes the size of the startup volume, so Retrospect may show the startup volume twice in the Sources view following an upgrade to Lion or Mountain Lion. If this happens, remove the original volume from the Sources list and redefine any favorite folders.

If the disk containing the Recovery HD partition is repartitioned and erased with an application like Disk Utility, or if a new hard drive is installed, the Recovery HD partition will no longer be present. Running the Mac OS X installer on this disk will recreate the Recovery HD partition.

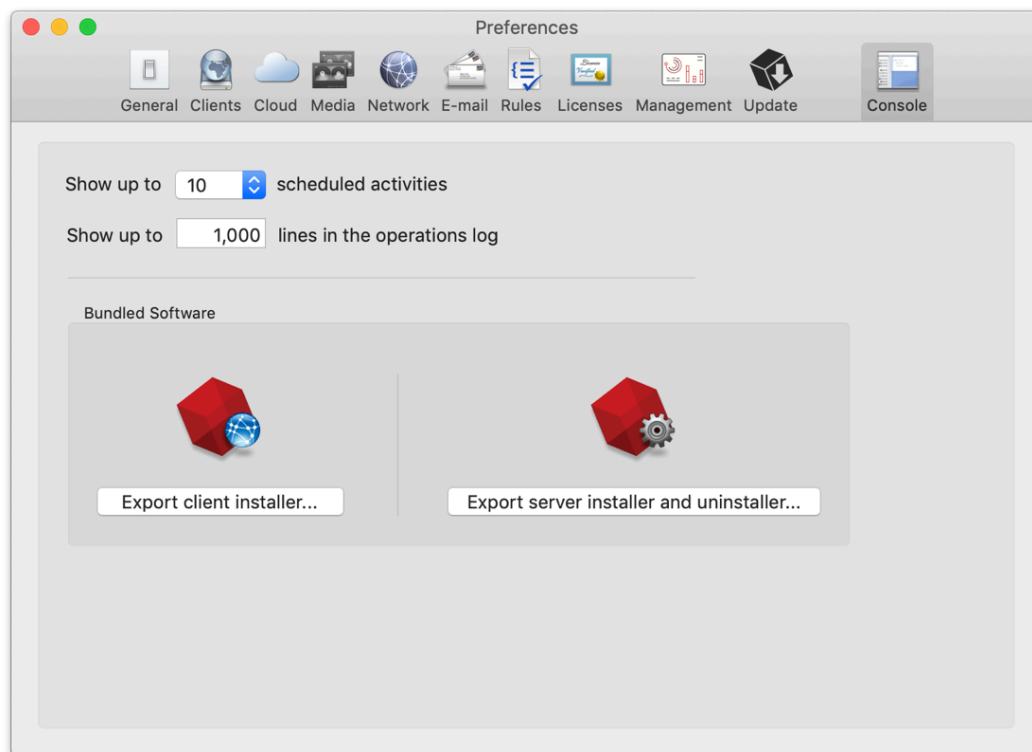
Managing Retrospect

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.

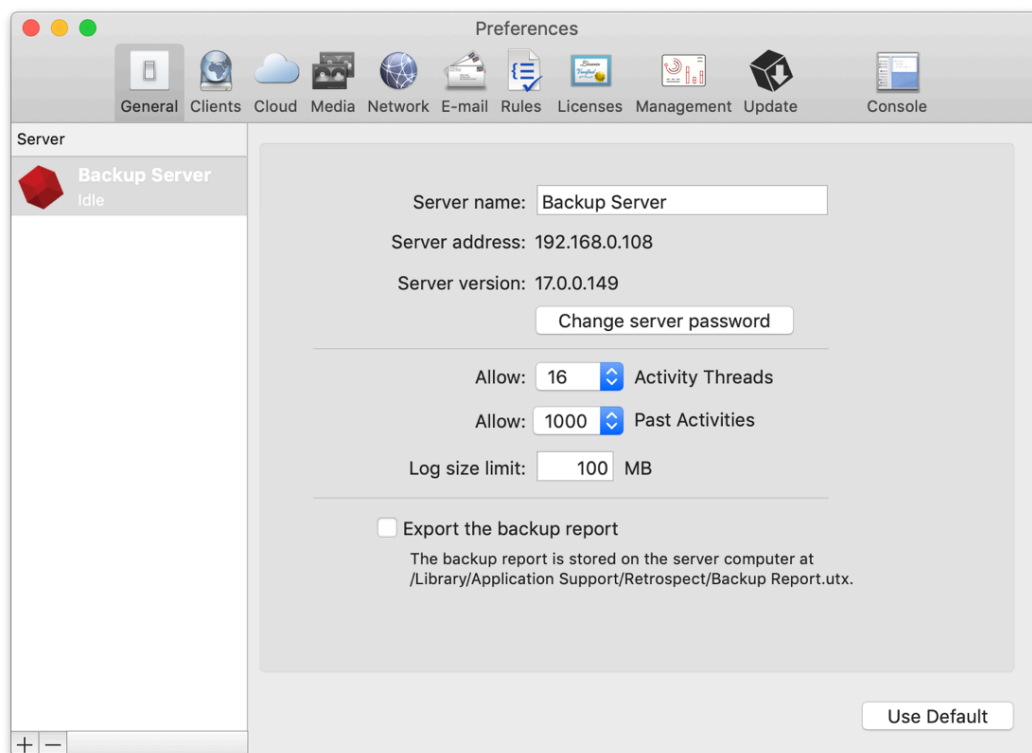
Show up to *n* scheduled activities controls the number of upcoming activities that appears in the

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.

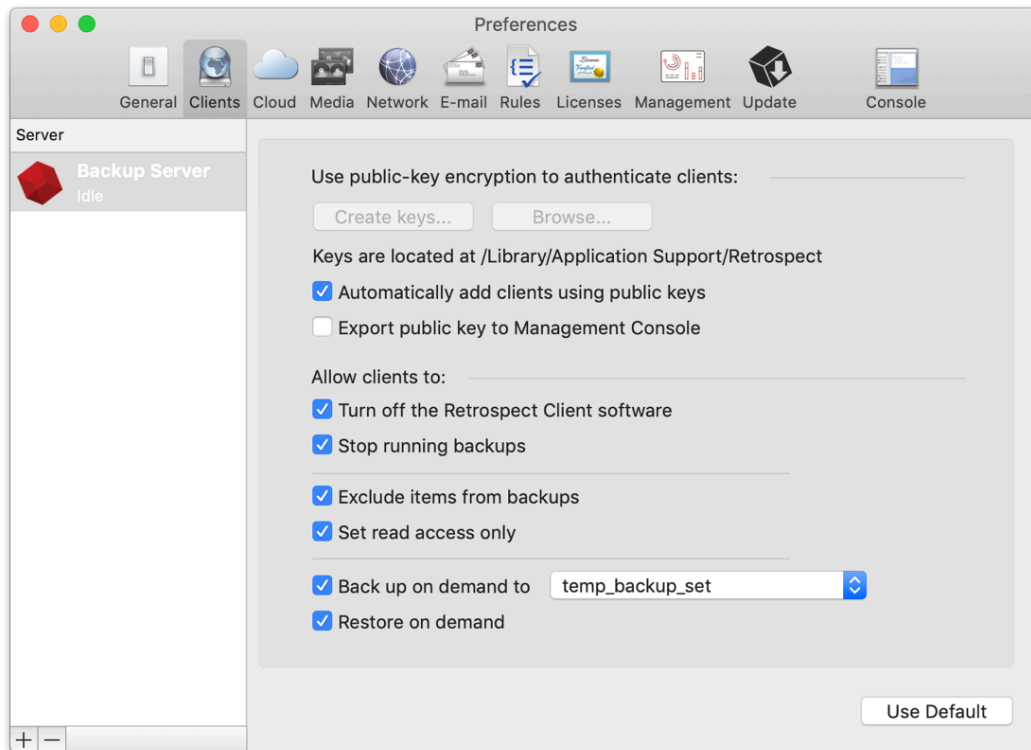
Log size limit allows you to set a number, in megabytes, for the size of the Operations Log. The default setting is 10 MB. When the log reaches the limit, the oldest portion of the log is deleted to keep its size within the limit. The bigger the log is, the longer it will take to open. Type the maximum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

Export the backup report allows you to save a copy of the backup report to a specific location on the server computer.

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:

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.

Upload it to Retrospect Management Console with the “Export public key to Management Console” checkbox.

If you want Retrospect to automatically log in clients with the proper public key, check “Automatically add clients”. This is recommended.

From the Retrospect disk image, open the Client Installers folder, then copy the Mac Client Installer folder onto your hard drive.

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.

Distribute or copy this public_key folder containing the pubkey.dat file along with the Retrospect Client installer.

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.

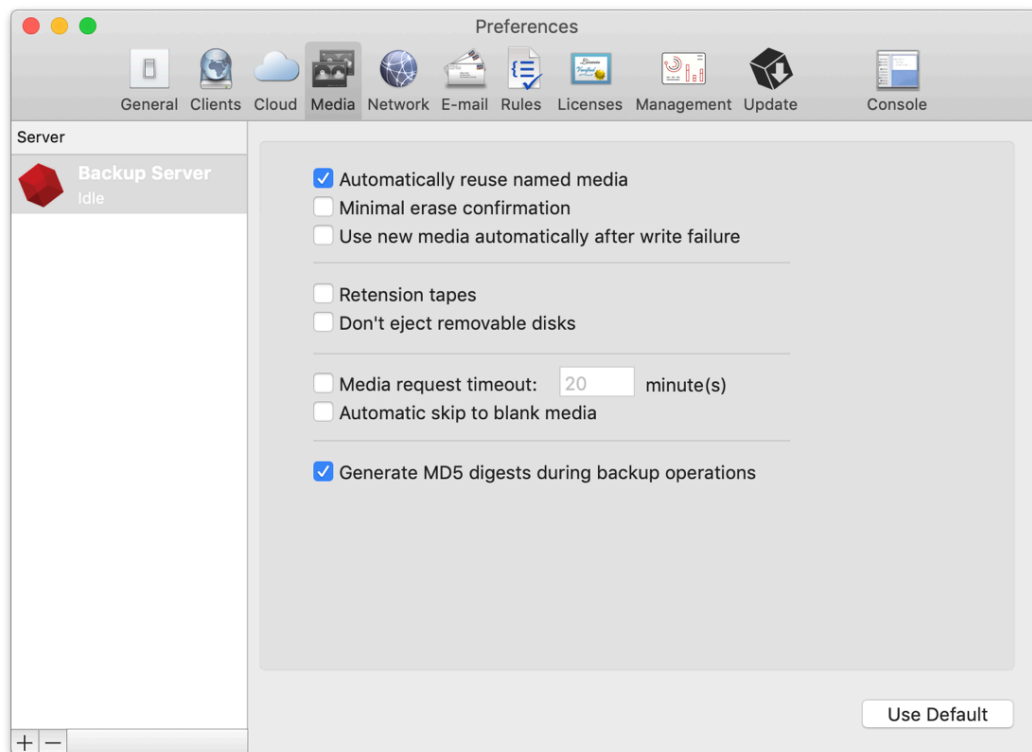
If keypair files already exist on the Retrospect server, you may load them by clicking the Browse button, then navigating to the folder that contains the two keypair files, then clicking Select. This can be used to share the same keypair files between multiple Retrospect backup engines.

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.

Retention 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.

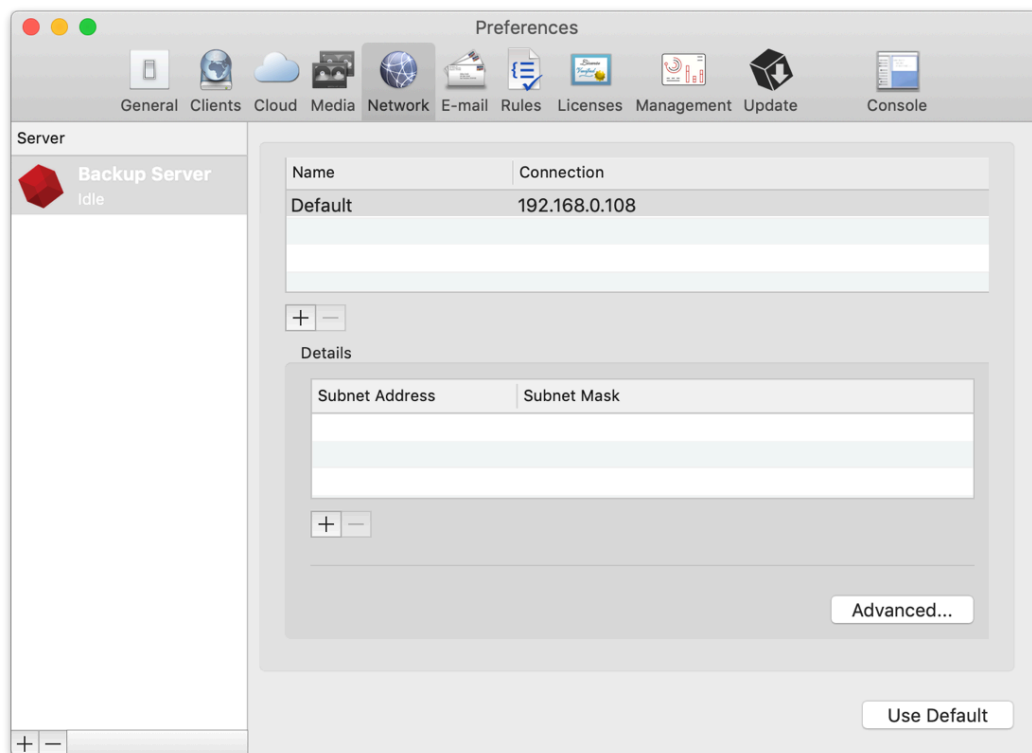
Media request timeout: *n* minutes sets the amount of time that Retrospect will wait for media to become available during execution. For example, if you're using a tape autoloader, it may take several minutes for the device to find and load a particular tape in the Media Set. This preference is off by 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:

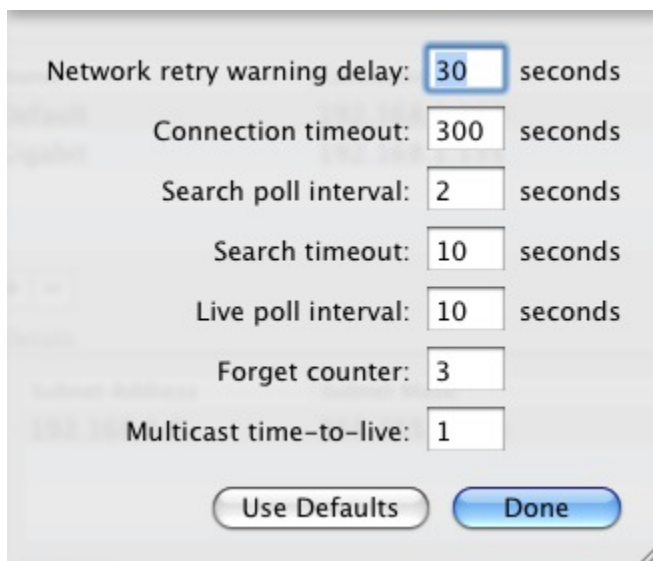
Choose Retrospect > Preferences > Network. If more than one Retrospect server appears in the Server column, select the server you want to control. In the connection list on the right side of the window, your Mac's default network connect will appear.

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

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:



Network retry warning delay: 30 seconds

Connection timeout: 300 seconds

Search poll interval: 2 seconds

Search timeout: 10 seconds

Live poll interval: 10 seconds

Forget counter: 3

Multicast time-to-live: 1

Use Defaults Done

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.

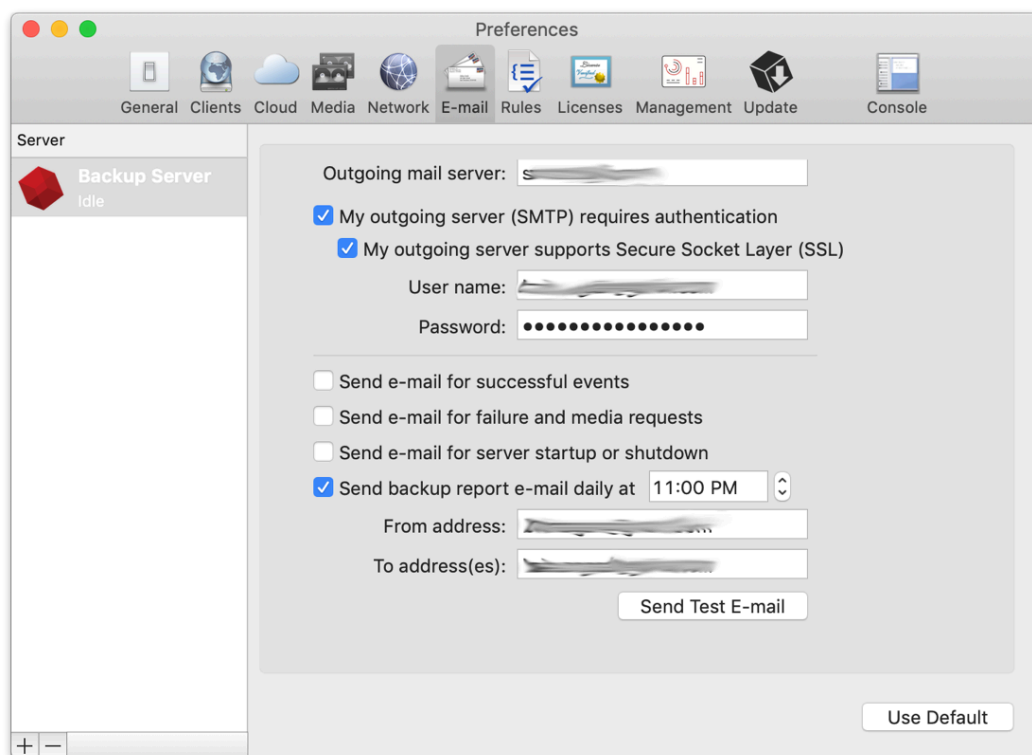
Multicast time-to-live Retrospect assigns this “time to live” number to multicast UDP packets. It is the maximum number of router hops a packet can make before it is discarded. An increase in the time to live number lets Retrospect search for clients on more subnets connected by IGMP capable routers. 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, [serverIpAdress]:[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.

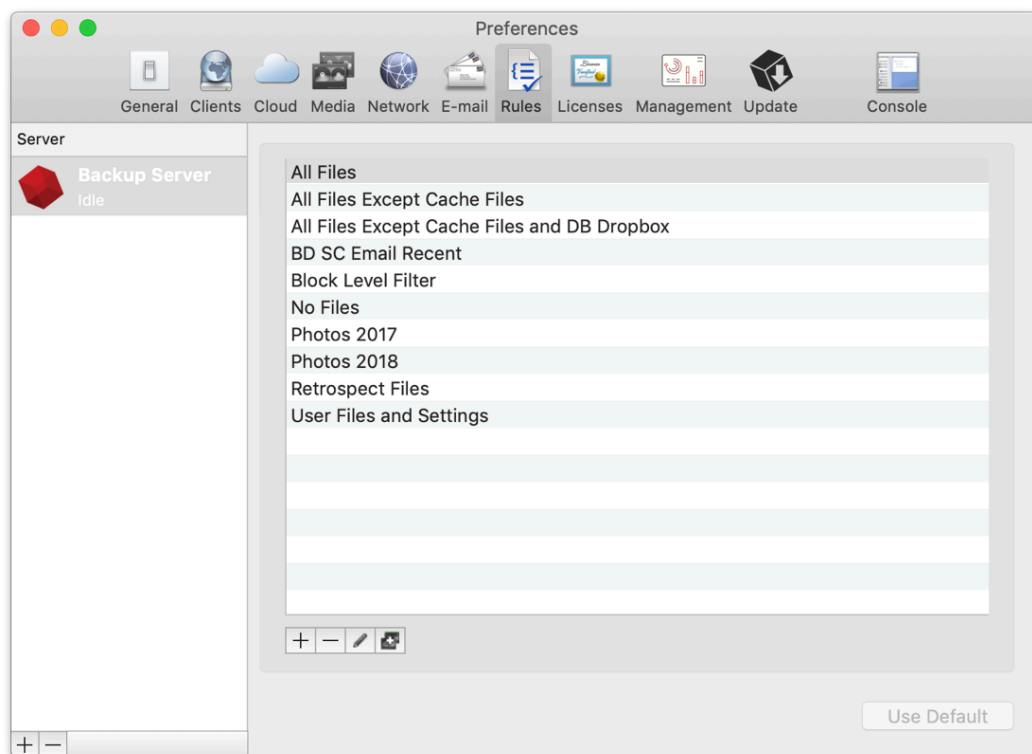
Send e-mail for successful events should be checked if you want Retrospect to notify you every time it completes a successful execution. Be aware, however, that if you have many scripts running, you may receive a large number of e-mails.

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.

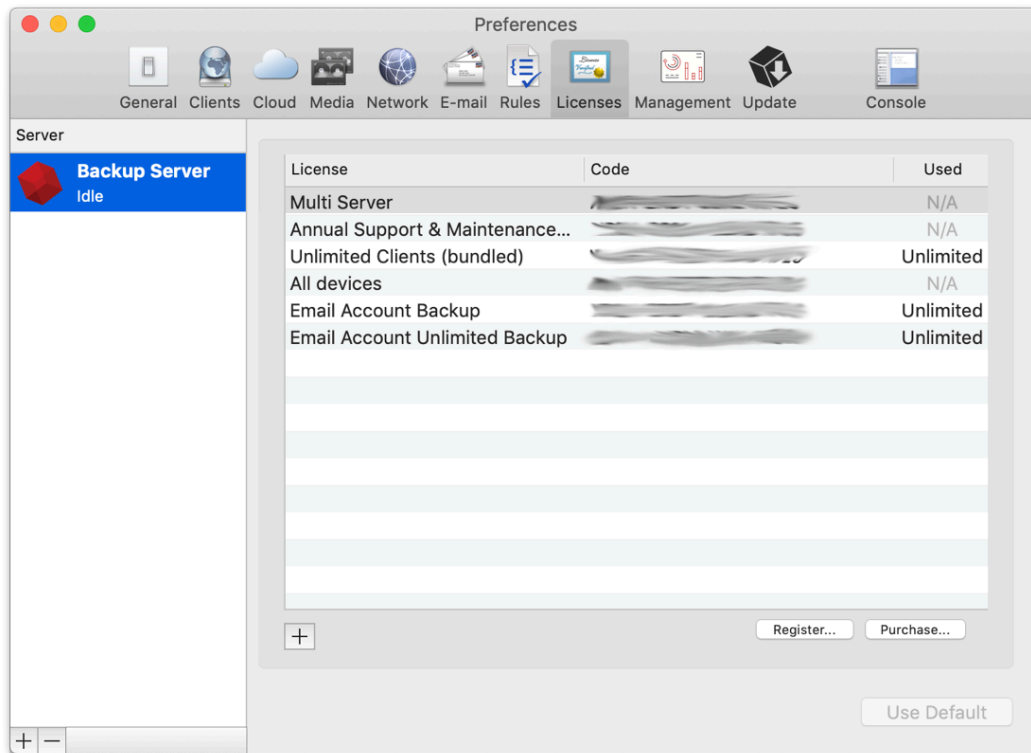
Rules Preferences

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.

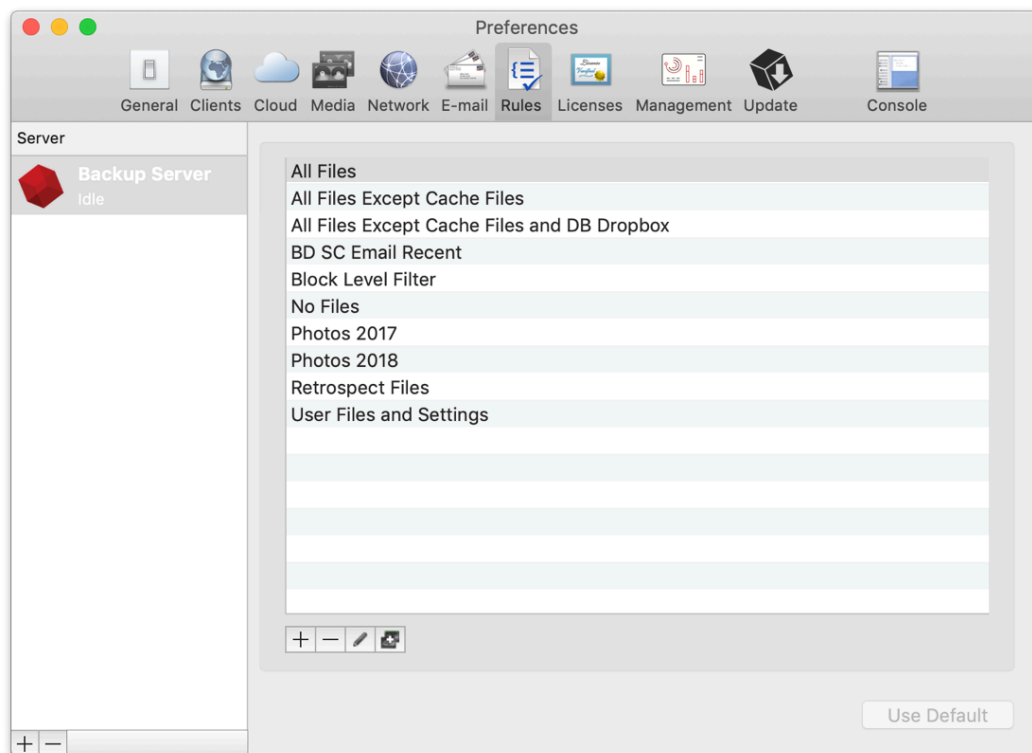
Retrospect comes with a number of Rules already set up for you. Rules are associated with each server separately, so if you have more than one Retrospect server, you can create different sets of Rules for each server. Simply click on the server in the sidebar of the preference pane to view the Rules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

Block Level Filter controls how a file is backed up, i.e. whether it is backed up in full or incrementally

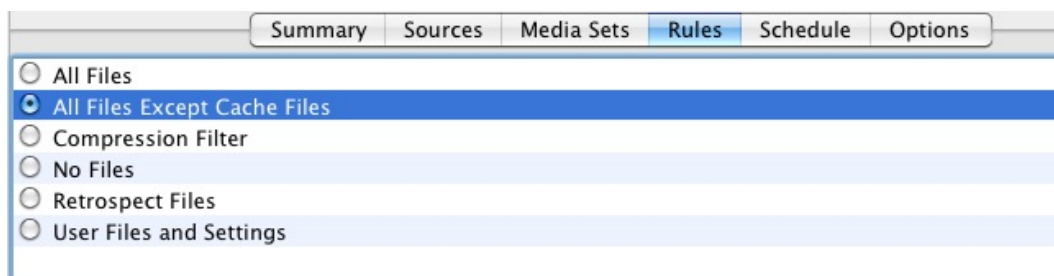
No Files does not mark any files for backup, though Retrospect will still save a complete file and folder listing and associated metadata for each source. Use the No Files rule for testing purposes when you don't want any files copied, or if you want to grab a System State-only backup of a Windows client.

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

Users Files and Settings marks files and folders inside the Mac OSX 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:

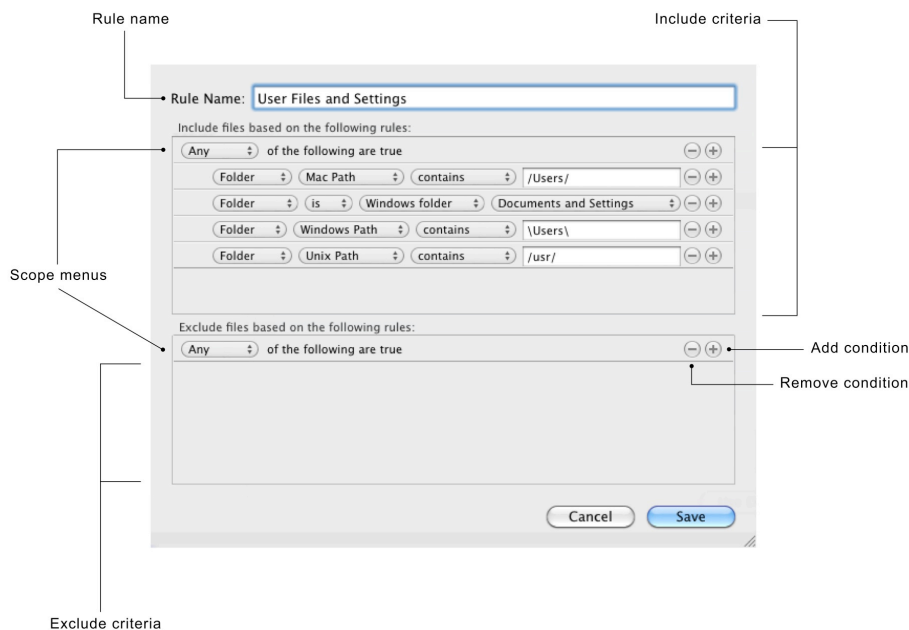
The **Rule name** can be anything you like. It will appear in the Rules tab of Preferences and Scripts, and will appear in other places within Retrospect.

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.



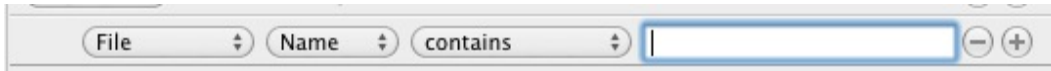
The All choice works as a logical *and* condition. For example, imagine that you want to backup all of the QuickTime movie files that are part of a particular project for your client Widgetco. You've previously saved all the movie files into a single folder. To add the All condition, hold down the Option 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.

For example, you could use "Folder" "Mac Path" "is like" `"/Volumes/*/Users/*/Library/*"` to include all libraries for every user from every volume.

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, an 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	Name
Folder	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 is 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 media via "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 ProactiveAI 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 ProactiveAI Backup scripts or regular Backup scripts.

Situations Suiting ProactiveAI 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 ProactiveAI Backup scripts. For example, you might choose to create ProactiveAI 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:

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.

In the Scripts category, create a new Backup script.

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.

In the script's Media Sets tab, click the checkboxes next to all five of the destination Media Sets that you created.

In the script's Rules tab, choose the Rule that you want to apply to the backups.

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.

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.

Basic ProactiveAI Backup

Create a ProactiveAI 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.

ProactiveAI 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 ProactiveAI 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 than 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 `configs.xml`. You should back up both of these files regularly. If your active configuration file (`Config80.dat`) becomes corrupt, stop the Retrospect engine, delete the `Config80.dat` file, then start the Retrospect engine, which creates a new `Config80.dat` from `configs.xml`.

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

In the sidebar, click Sources.

In the Sources list, click to select the hard disk of the Retrospect backup server.

Click the Browse button. Retrospect will display a browse dialog showing the contents of the Retrospect backup server’s hard disk.

Navigate to, then click to select `/Library/Application Support/Retrospect/`.

At the bottom of the browse dialog, click Add to Favorite Folders, then click Done.

In the sidebar, click Media Sets, then above the Media Sets list, click the Add button. Retrospect displays the Media Set dialog.

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.

In the sidebar, click Scripts, then above the Scripts list, click the Add button. Retrospect displays the Script dialog.

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.

In the detail area, click the Sources tab, then click the checkbox next to the Retrospect Favorite Folder you just created.

Click the Media Sets tab, then click the checkbox next to the name of the Media Set you created.

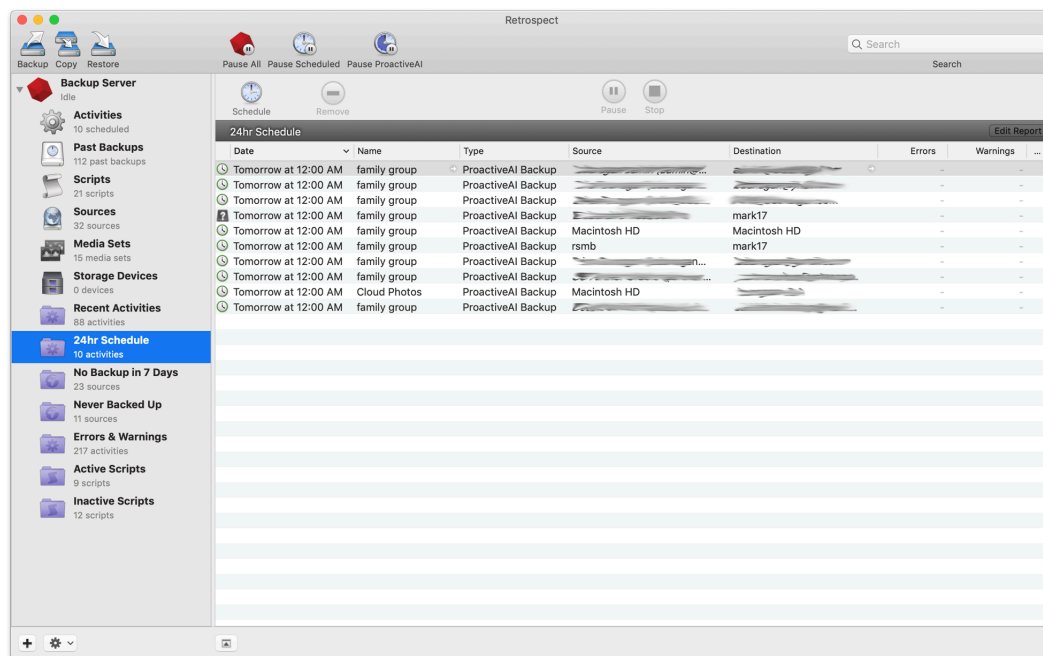
In almost all cases the default Rule of All Files will be what you want, so skip the Rules tab and click the Schedule tab. Add one or more Schedules to backup the Catalog and configuration files. As one possibility, you could create one schedule that executes every day at a particular time with no media 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.

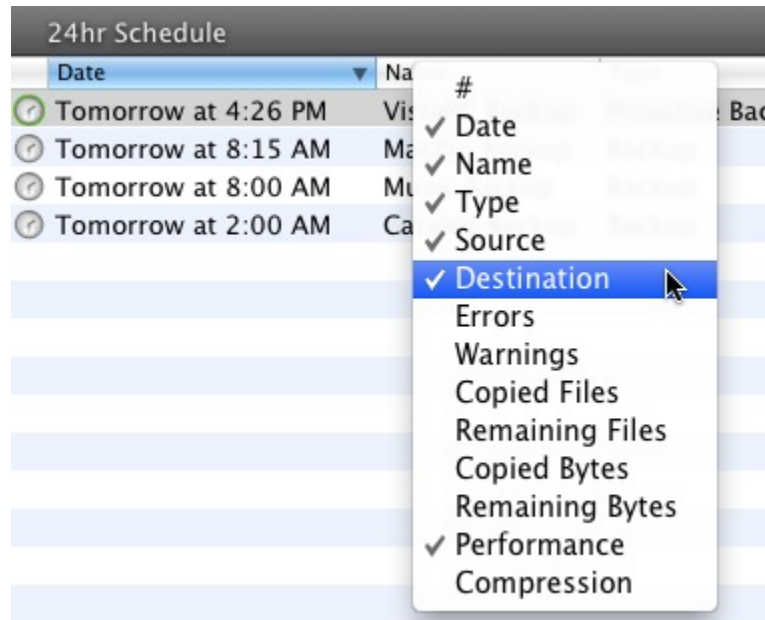
To view a report, click on one of the report names in the sidebar. The main part of the Retrospect window changes to display the report.



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.

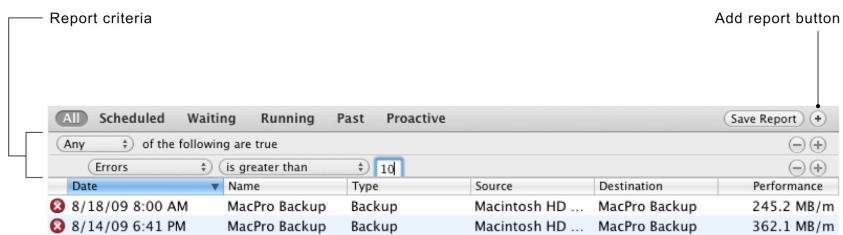


Creating and Saving Reports

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.

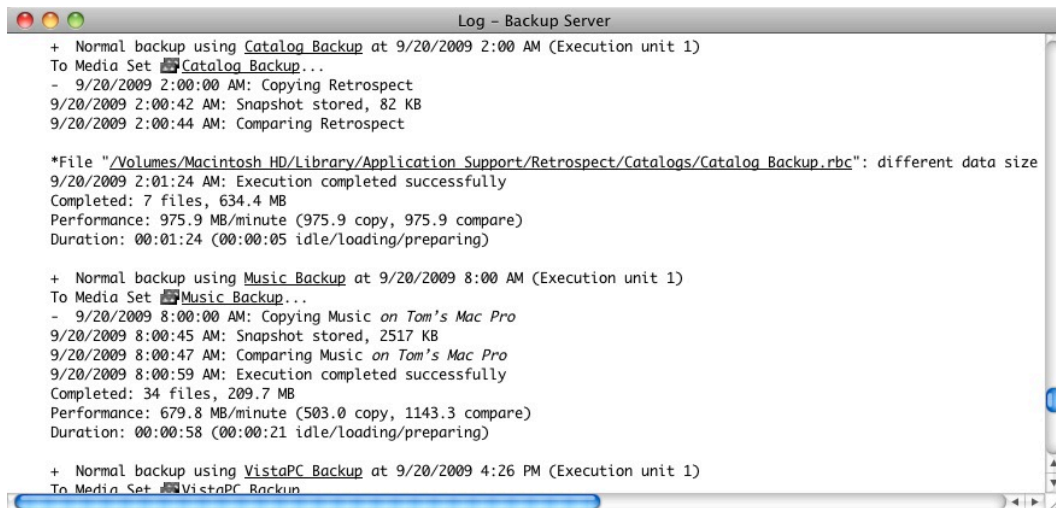
To duplicate a report, perhaps because you wish to use it as the base for a new report, right-click on the report's name in the sidebar, and choose Duplicate Report from the resulting contextual menu. Retrospect displays a dialog asking you to name the new report. Enter the name, then click OK. Then 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 keeps 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:

- Select the Media Set you wish to verify, then click the Verify button in the Media Set toolbar.

- 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:

Select the Media Set you want to repair in the Media Set list.

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.

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.”

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.

Click to select the Media Set member in the dialog, then click Next. The Media Set member appears in the Repair dialog.

If there are additional members of the Media Set you need to add, repeat steps 3 through 5 until all members have been added.

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:

Select the Media Set you want to rebuild in the Media Set list.

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.

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.

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."

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.

Click to select the Media Set member in the dialog, then click Next. The Media Set member appears in the Rebuild dialog.

If there are additional members of the Media Set you need to add, repeat steps 4 through 6 until all members have been added.

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.

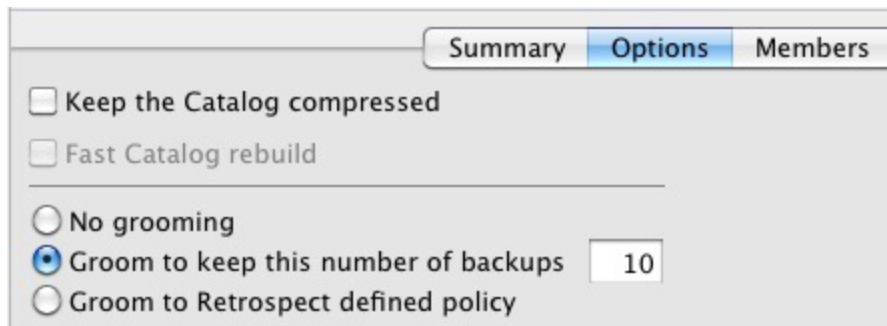
If you would rather continue to use the existing disk, you can use Retrospect's grooming options to reclaim disk space by deleting older files and folders to make room for new ones.

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:

Select the Media Set you want to recycle in the Media Set list.

Click the Recycle button in the Media Set toolbar. Retrospect displays a dialog asking you to confirm the choice. Click Recycle.

Because the recycle will result in data loss, Retrospect asks you to confirm the operation again. Click Cancel or Recycle.

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:

Install the Retrospect engine and console on the new computer.

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:

On the new Retrospect server, use the Retrospect system preference pane to stop the Retrospect engine.

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.

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:

Use the Retrospect system preference pane to start the Retrospect engine on the new Retrospect server.

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.

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.

Uninstalling Retrospect

To remove Retrospect for Mac, follow the steps outlined below.

The Uninstaller preserves Config files (which contain the database of logged-in clients, scripts and schedules, and general Retrospect engine preferences), the Retrospect console's preferences, and all Media Set Catalog files (which keep track of what files are backed up to each Media Set). If you instead want to completely remove all of these settings and Catalogs, delete the following files and folders:

```
/Library/Application Support/Retrospect/Catalogs/  
  
/Library/Application Support/Retrospect/Config80.bak  
  
/Library/Application Support/Retrospect/Config80.dat  
  
/Library/Application Support/Retrospect/ConfigISA.bak  
  
/Library/Application Support/Retrospect/ConfigISA.dat  
  
/Library/Application Support/Retrospect/retro_isa.ini  
  
/Library/Application Support/Retrospect/retro.ini  
  
~/Library/Preferences/com.Retrospect.plist
```

Open the Retrospect application folder and double-click the Uninstall Retrospect icon to run the uninstaller.

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:

Make sure all instances of the Retrospect console are closed, whether those are on the Retrospect server machine or on a remote machine.

From the Apple menu, choose System Preferences > Retrospect.

In the System Preferences window, click Retrospect.

In the Retrospect preference pane, click the lock in the lower-left corner, then enter your

administrator password and click OK.

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.

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:

Make sure that the Retrospect engine is actually running on the Retrospect server.

Make sure that the Retrospect server machine’s networking is correctly configured.

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:

Click Sources in the console’s sidebar, then click the Add button in the Sources view’s toolbar. The Add Sources dialog appears.

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.

On the Retrospect client machines

If a client machine does not appear in the Retrospect console:

Open the Retrospect Client control panel on the client computer and check whether the client software was loaded at startup and whether it is turned on. Check that its status field says “Ready”

or “Waiting for first access.”

Make sure the 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:

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.

Retrospect Management Console

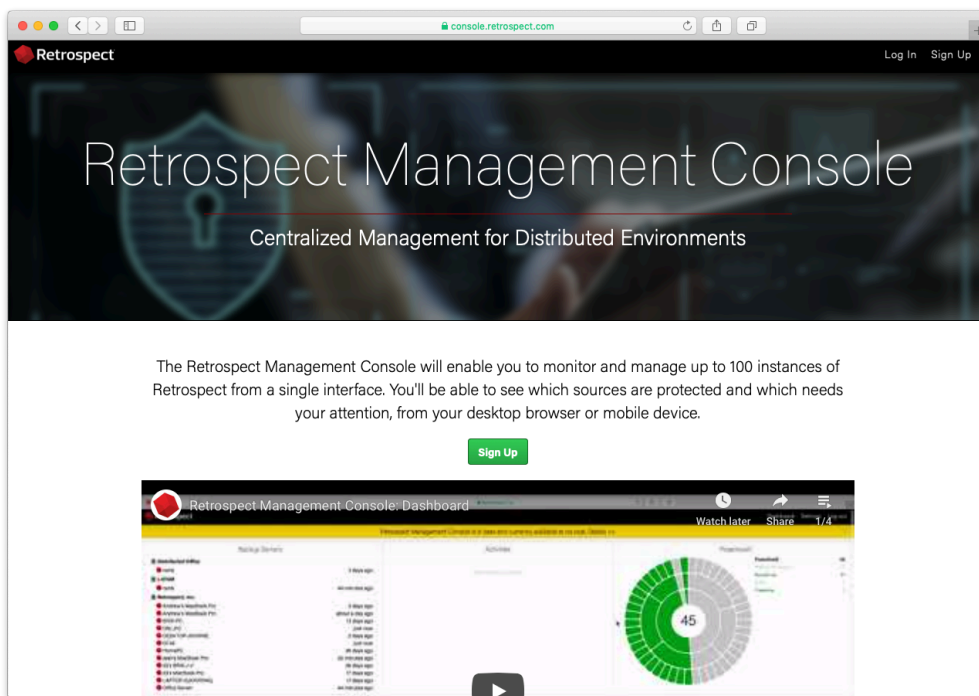
Retrospect Management Console enables you to monitor and manage multiple instances of Retrospect from a single interface. You'll be able to see which sources are protected and which needs your attention, from your desktop browser or mobile device. Retrospect Backup 16 for Windows or Mac is required.

Retrospect Management Console enables complete monitoring and management available from anywhere for every Retrospect Backup engine. It is a hosted service with in-transit and at-rest encryption, enabling businesses and partners to securely monitor and manage their backup environment. [See details.](#)

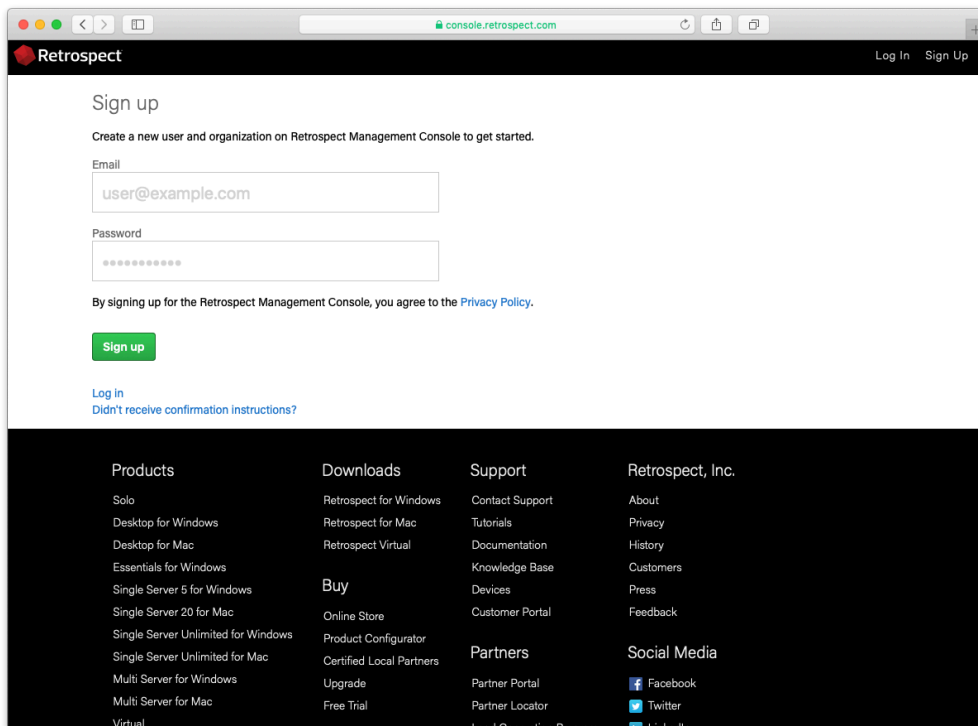
We will walk through integrating Retrospect Backup with Retrospect Management Console.

Account Creation

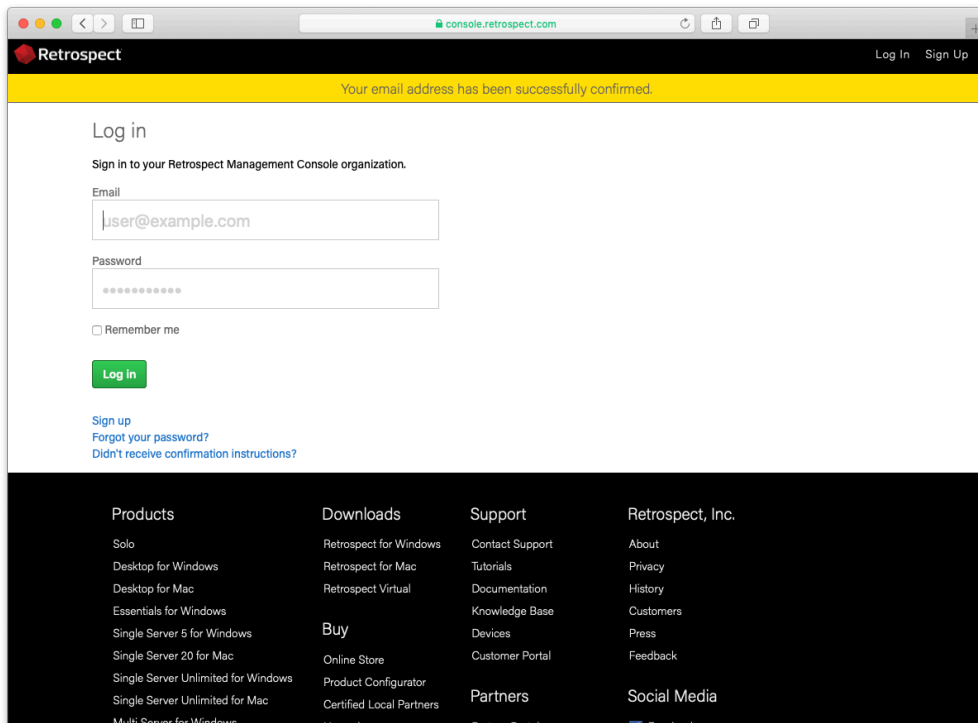
Go to <https://console.retrospect.com>. Select on "Sign Up".



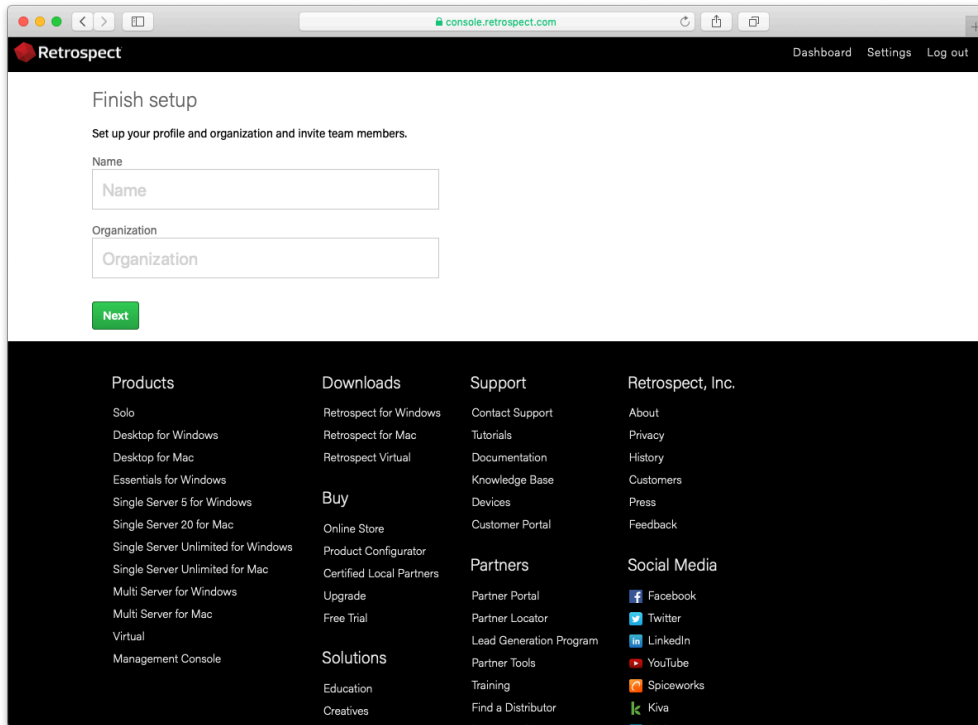
Type in your email and password and click "Sign Up"



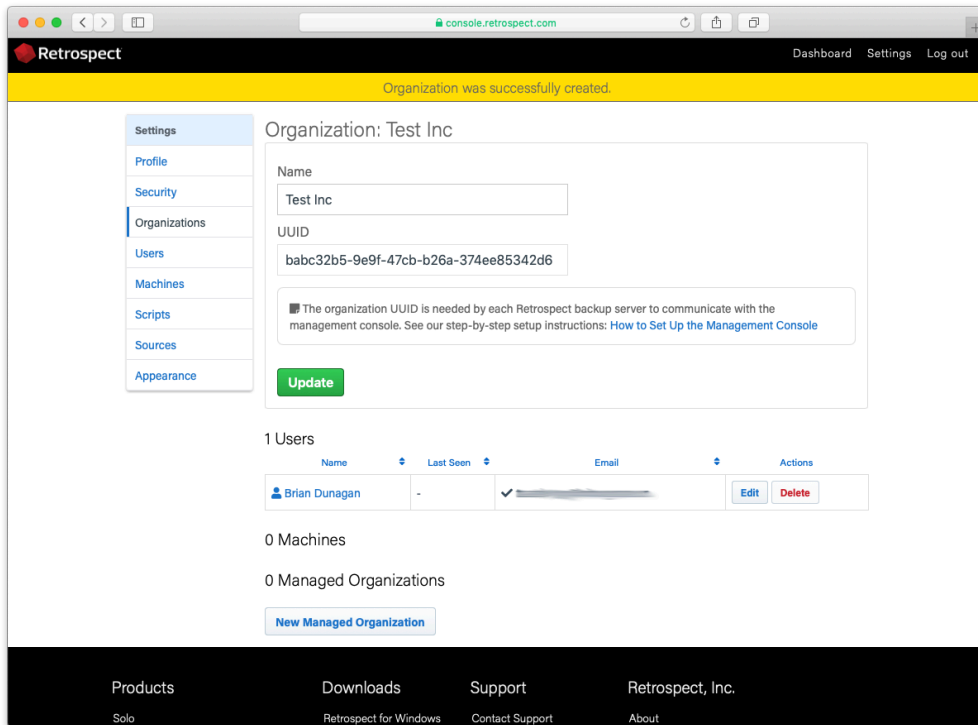
When you sign up, we generate a verification email to ensure you are the owner of that email address. Select on the link in the email to verify it.



Type in your name and organization.



Your organization is now created.

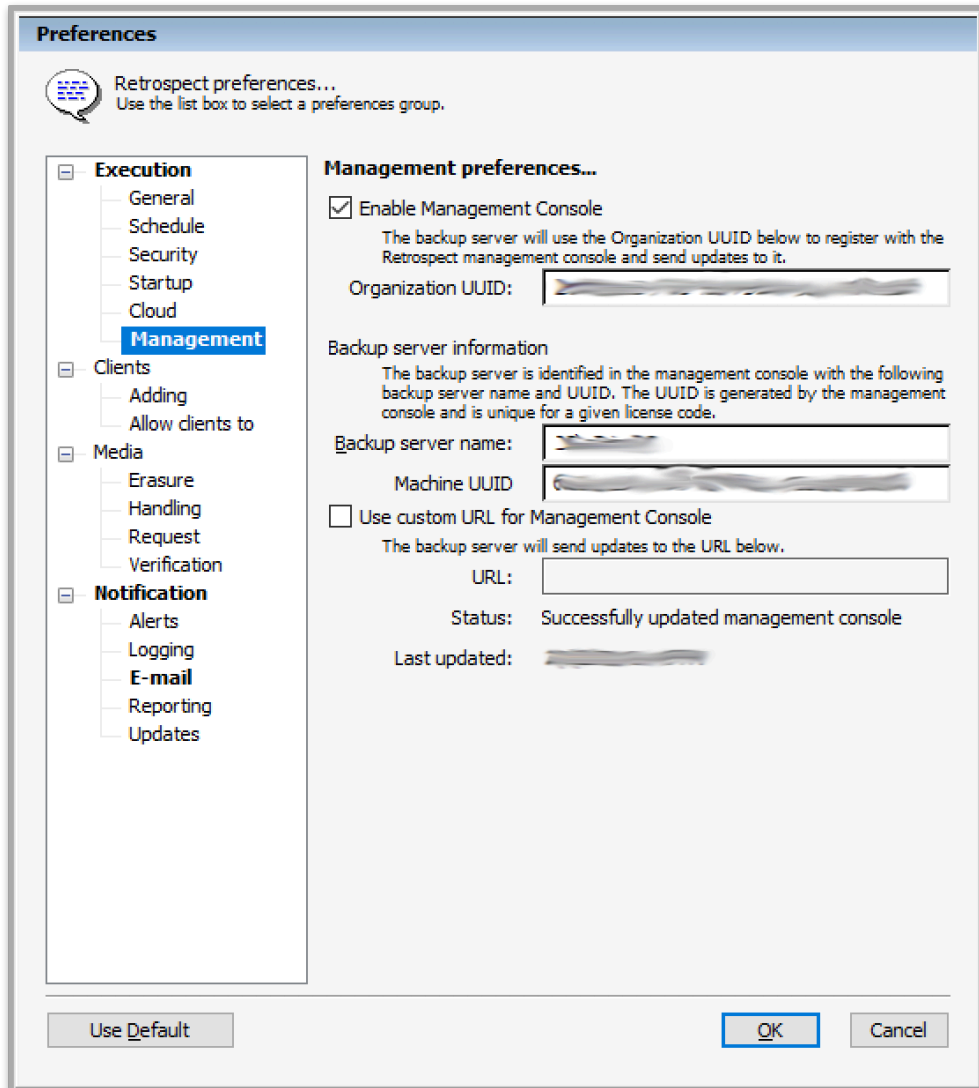


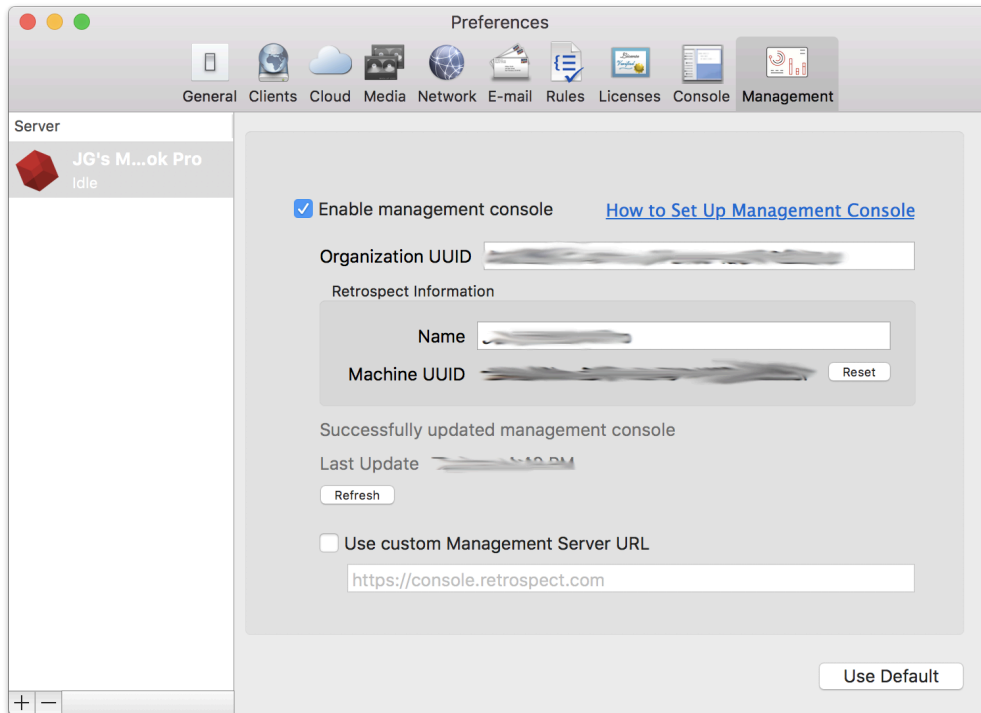
System Setup

Install Retrospect 16.

Ensure that the application has a license.

Navigate to the Preferences. On Windows, it's available on the left navigation. On Mac, it's available in the toolbar menu.





Select "Management".

Check "Enable Management Console" and fill in the "Organization UUID" from your Retrospect Management Console settings and the server name if not already filled in.

Close Preferences. The engine data will show up in your Retrospect Management Console account, and you'll see the "Last Updated" status show the last time the data was sent. There is also a status message to help troubleshooting.

If you receive the error "The management console requires an organization UUID and so the option was turned off." on Windows, please check that you added both the Organization UUID and the backup server name.

Firewall Configuration

Retrospect Backup communicates with the Management Console using HTTPS, so the port is 443. As it's the same as HTTPS web traffic (like Gmail and Amazon), it's not generally blocked. If the firewall white-lists domains, "console.retrospect.com" will need to be added.

Technical Details

The Retrospect Management Console uses the organization UUID to link a Retrospect Backup instance to the correct organization. Within the organization, the Retrospect Backup application license is used to uniquely identify the data for that instance. If the application license is used by more than one instance (for example, re-using a trial license), then the data from the most recent communication from one of those instances will appear.

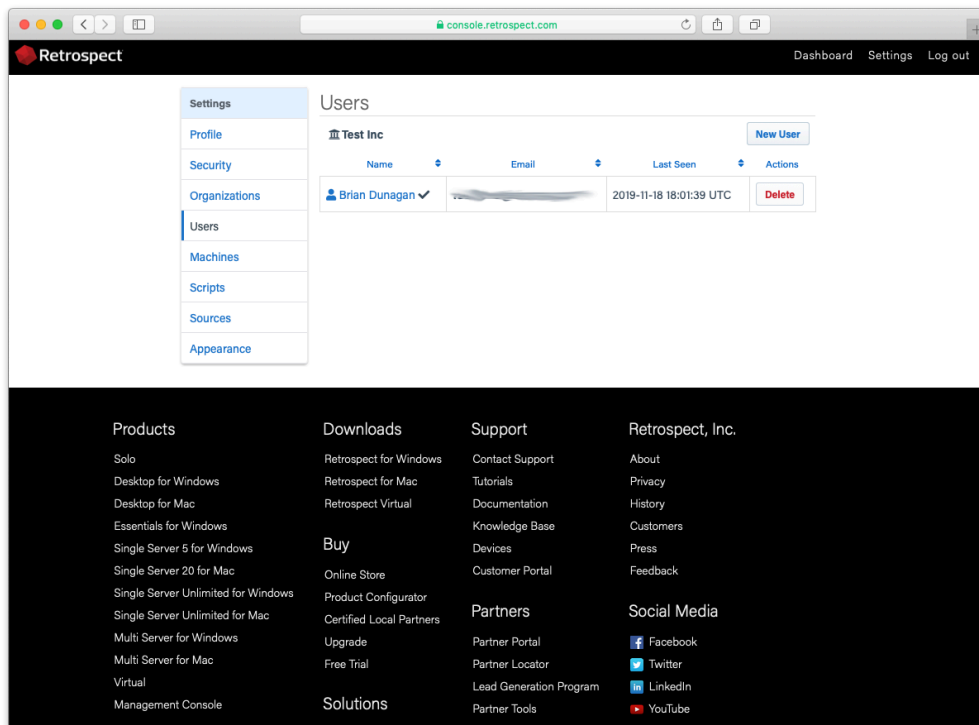
When configured, Retrospect Backup communicates with the Retrospect Management Console every minute.

To disable it, repeat the above steps and uncheck "Enable Management Console".

User Creation

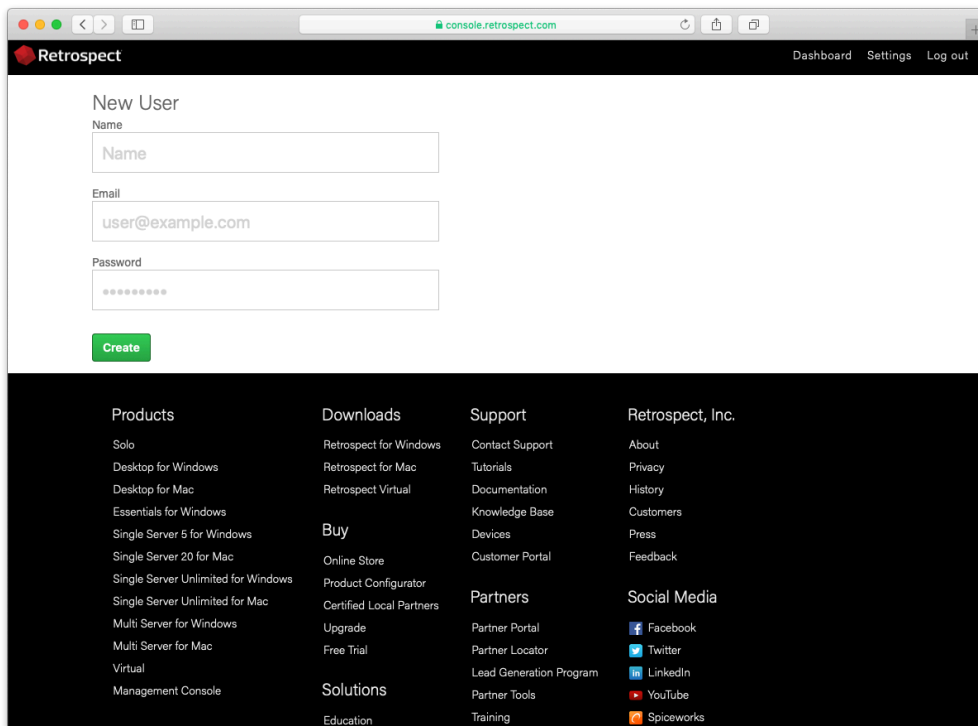
Select "Settings" in the top right.

Select "Users".

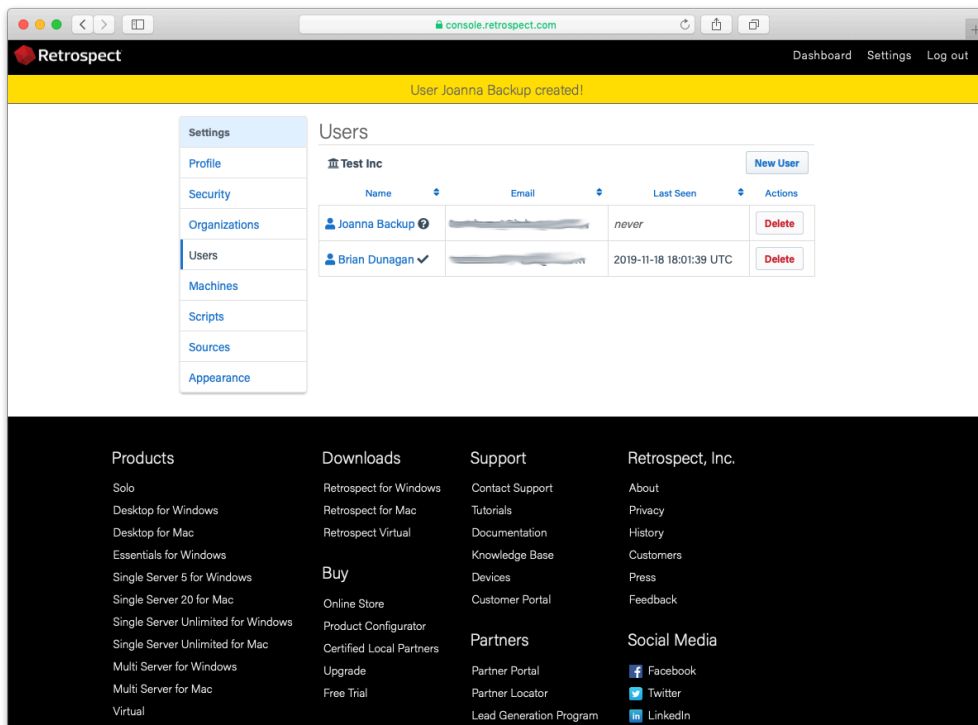


Select "New User".

Type in the name, email, and password. Select "Create".



Your user is now created.



Organization Creation

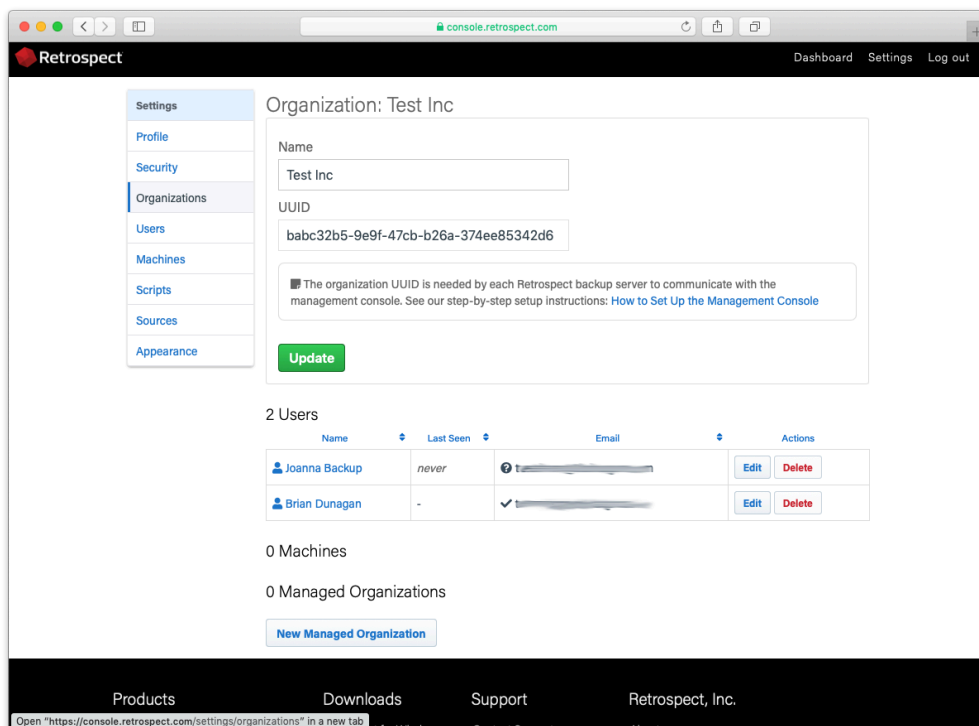
Retrospect Management Console allows you to managed multiple managed organizations within your organization. This might be in the form of different geographic sites where you have a number of

Retrospect Backup engines, or it might be a partner managing different customer accounts. There is no limitation on the number of organizations that you can manage or the managed organization can manage.

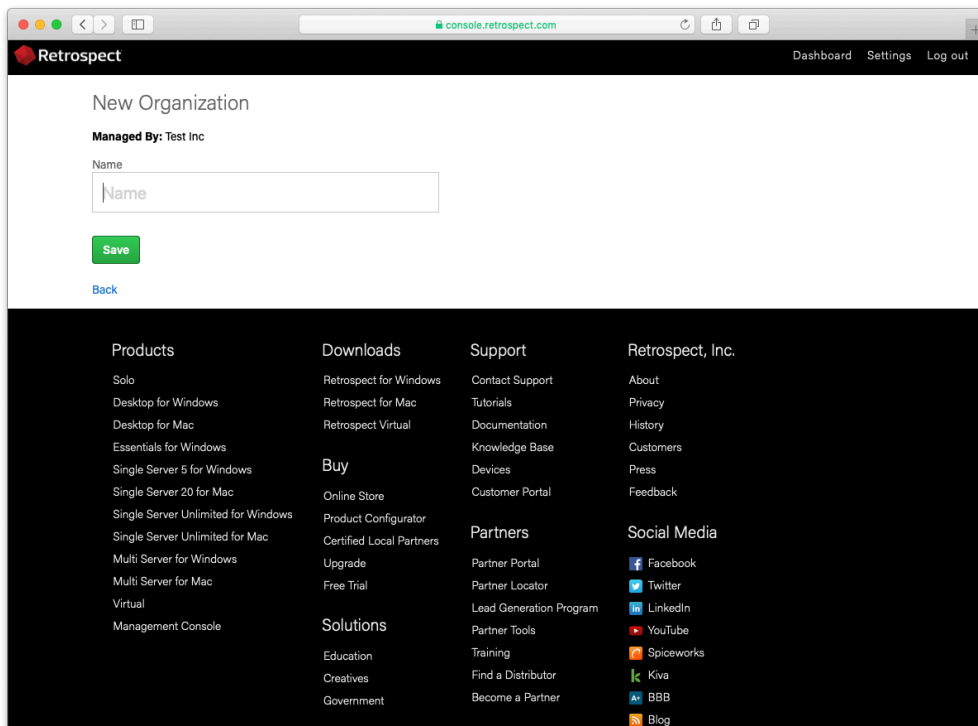
Select "Settings" in the top right.

Select "Organizations" on the left.

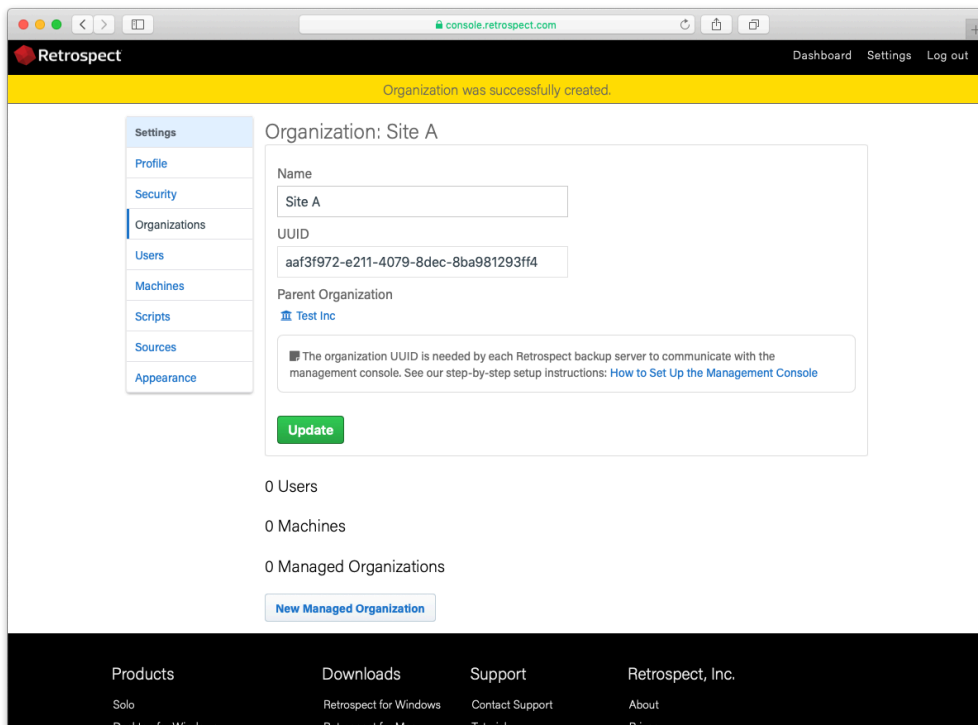
Select "New Managed Organization" at the bottom.



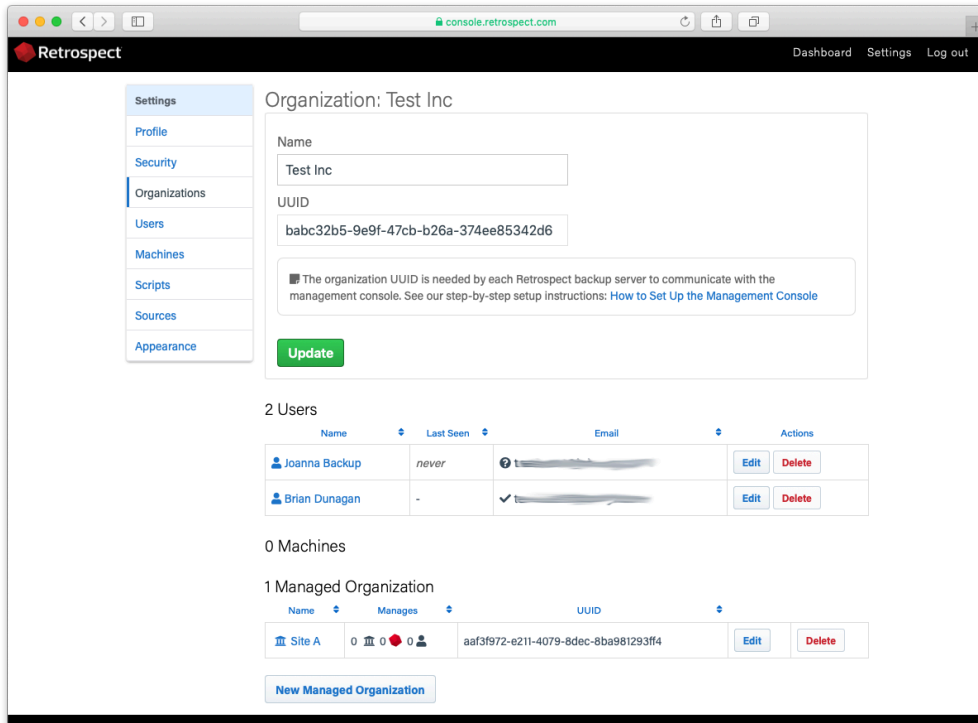
Type in the new managed organization's name and select "Save".



Your new managed organization is created. You will see their new UUID.



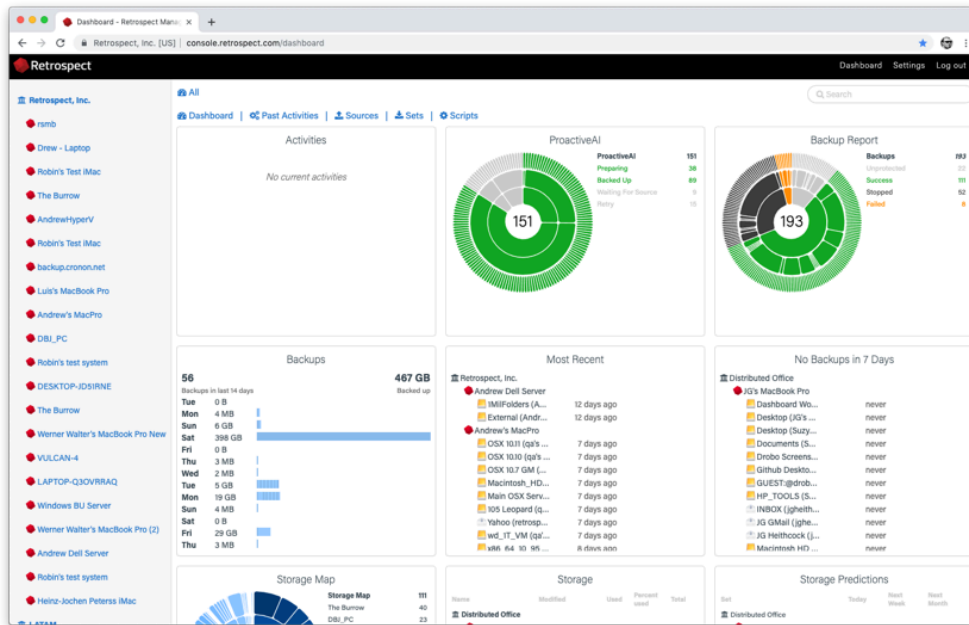
Select "Organizations" to see a list of your managed organizations.



Overview

Retrospect Management Console displays activities, sources, and backup sets for customers to drill down on.

Dashboard



Activities

Retrospect console showing the 'Activities' page. The page displays a list of backup jobs across various sources, including 'Distributed Office' and 'Retrospect, Inc.'.

Name	Source	Destination	Script	Status	File Copied	File Remaining	Copied	Remaining
Distributed Office								
● JG's MacBook Pro								
Nuther test			Nuther test	Execution incomplete	0	0	0.00 B	0.00 B
Nuther test			Nuther test	Execution incomplete	0	0	0.00 B	0.00 B
■ Retrospect, Inc.								
● Andrew Dell Server								
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-35 on Data1 (D)		Execution completed succe...	Execution completed succe...	3	0	179 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-50 on Data1 (D)		Execution completed succe...	Execution completed succe...	18	0	230 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-51 on Data1 (D)		Execution completed succe...	Execution completed succe...	19	0	218 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-36 on Data1 (D)		Execution completed succe...	Execution completed succe...	4	0	180 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-37 on Data1 (D)		Execution completed succe...	Execution completed succe...	5	0	184 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-38 on Data1 (D)		Execution completed succe...	Execution completed succe...	6	0	186 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-39 on Data1 (D)		Execution completed succe...	Execution completed succe...	7	0	188 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-40 on Data1 (D)		Execution completed succe...	Execution completed succe...	8	0	190 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-41 on Data1 (D)		Execution completed succe...	Execution completed succe...	9	0	192 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-42 on Data1 (D)		Execution completed succe...	Execution completed succe...	10	0	199 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-39 on Data1 (D)		Execution completed succe...	Execution completed succe...	27	0	264 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-40 on Data1 (D)		Execution completed succe...	Execution completed succe...	28	0	249 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-43 on Data1 (D)		Execution completed succe...	Execution completed succe...	11	0	197 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-61 on Data1 (D)		Execution completed succe...	Execution completed succe...	29	0	272 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-62 on Data1 (D)		Execution completed succe...	Execution completed succe...	30	0	255 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-63 on Data1 (D)		Execution completed succe...	Execution completed succe...	31	0	257 KB 0.00 B
BAT.BUJLongMul...	BATdiskset_none_4_thrd_4	BAT_thrd_4-44 on Data1 (D)		Execution completed succe...	Execution completed succe...	12	0	199 KB 0.00 B

Sources

Retrospect console showing the 'Sources' page. The page displays a list of backup sources, including 'Distributed Office' and 'Retrospect, Inc.'.

Name	Machine	Used	Free	Total	Last Backup
Distributed Office					
● JG's MacBook Pro					
Dashboard Work on Macintosh HD	JG's MacBook Pro	464 GB	1.70 GB	466 GB	-
Desktop on Suzy's HD	Suzys iMac	2.19 TB	664 GB	2.84 TB	-
Desktop on Macintosh HD	JG's MacBook Pro	464 GB	1.70 GB	466 GB	-
Documents on Suzy's HD	Suzys iMac	2.19 TB	664 GB	2.84 TB	-
Drobo Screenshots on Macintosh HD	JG's MacBook Pro	464 GB	1.70 GB	466 GB	-
GitHub Desktop Welcome Wizard sc...	JG's MacBook Pro	464 GB	1.70 GB	466 GB	-
GUEST@drobot92/Public	JG's MacBook Pro	197 GB	63.7 TB	63.9 TB	-
HP_TOOLS	Sharlees-HP	2.48 MB	1.99 GB	1.99 GB	-
INBOX on jgheilthcock@gmail.com	JG's MacBook Pro	0.00 B	8.00 EB	8.00 EB	-
JG Gmail (jgheilthcock@gmail.com)	JG's MacBook Pro	0.00 B	8.00 EB	8.00 EB	-
JG Heilthcock (jgheilthcock@retros...	JG's MacBook Pro	0.00 B	8.00 EB	8.00 EB	-
Macintosh HD	Kitchen iMac	781 GB	1.06 TB	1.82 TB	-
Macintosh HD	JG's MacBook Pro	459 GB	6.30 GB	466 GB	-
Macintosh HD	Morgan Heilthcock's MacBook	364 GB	102 GB	466 GB	-
Mac SSHD	Kitchen iMac	624 GB	307 GB	931 GB	-
Recovery	Suzys iMac	2.18 TB	670 GB	2.84 TB	-
Recovery Image	Sharlees-HP	13.3 GB	1.98 GB	15.3 GB	-
ROVI	Sharlees-HP	1.99 GB	1.80 GB	3.80 GB	-
Suzy's HD	Suzys iMac	2.19 TB	664 GB	2.84 TB	-
Test	JG's MacBook Pro	5.07 TB	56.9 TB	63.9 TB	-
Web on Macintosh HD	JG's MacBook Pro	464 GB	1.70 GB	466 GB	-

Backup Sets

The screenshot shows the Retrospect Management Console interface. The left sidebar lists various engines under 'Retrospect, Inc.', including 'ramb', 'Drew - Laptop', 'Robbi's Test iMac', 'The Burrow', 'AndrewHyperV', 'Robbi's Test iMac', 'backup.cronon.net', 'Lui's MacBook Pro', 'Andrew's MacPro', 'DBU_PC', 'Robbi's test system', 'DESKTOP-JDSIRNE', 'The Burrow', 'Werner Walter's MacBook Pro New', 'VULCAN-4', 'LAPTOP-Q3QVRRAQ', 'Windows BU Server', 'Werner Walter's MacBook Pro (2)', 'Andrew Dell Server', 'Robbi's test system', and 'Heinz-Jochen Peterss iMac'. The main area displays a table of sets for 'Distributed Office' and 'Retrospect, Inc.' engines.

Name	Type	Used	Free	Capacity	Files	Members	Last Backup
Distributed Office							
JG's MacBook Pro							
Cloud Set A	Cloud	0.00 B	0.00 B	0.00 B	0	0	8/16/2019, 2:33:18 PM
Disk Set A	Disk	0.00 B	0.00 B	0.00 B	0	0	8/16/2019, 2:34:06 PM
Media Set A	Disk	21.7 GB	4.94 MB	21.7 GB	286930	1	8/29/2019, 1:09:54 AM
Media Set Asd	Cloud	0.00 B	0.00 B	0.00 B	0	0	8/20/2019, 7:10:46 PM
Morgan's Email	Disk	2.48 GB	7.79 GB	10.3 GB	12568	1	7/17/2019, 8:18:06 PM
Retrospect, Inc.							
Andrew Dell Server							
BATS3_none_0-Administrator-192-L...	Cloud	156 MB	0.00 B	156 MB	11	1	8/2/2019, 9:37:02 PM
CAPtest	Tape	0.00 B	0.00 B	0.00 B	0	0	5/7/2019, 2:23:00 PM
George SG BI	Disk	3.73 MB	763 GB	763 GB	1	0	5/8/2019, 9:34:51 AM
IMAP	Disk	10.2 GB	1.67 TB	1.68 TB	204594	1	9/24/2019, 12:14:28 PM
ISCSI	Disk	97.7 GB	7.29 GB	105 GB	200662	1	7/11/2019, 4:36:01 PM
LocalUseAtMostTest	Disk	1.40 GB	231 GB	232 GB	2935	0	4/5/2019, 4:49:21 PM
NASShareTest	Disk	1.46 GB	761 GB	762 GB	3087	1	4/5/2019, 5:05:56 PM
ShareTest	Disk	137 GB	625 GB	762 GB	253411	1	4/5/2019, 4:51:27 PM
ShareXMLTest	Disk	6.73 GB	638 GB	645 GB	4136	1	7/23/2019, 5:30:32 PM
TransferTest	Disk	138 GB	1.68 TB	1.82 TB	58002	1	7/23/2019, 5:34:37 PM
AndrewHyperV							
BATSkset_aes256-	Disk	115 GB	324 GB	325 GB	24500	1	3/1/2019, 4:30:44 PM
GnomTest	Disk	3.88 GB	1.36 TB	1.37 TB	59053	1	3/1/2019, 5:22:46 PM
HomeBU	Disk	3.64 TB	3.48 MB	3.64 TB	1235955	1	3/1/2019, 1:30:08 PM

Scripts

Retrospect Management Console also displays scripts (only available with Retrospect Backup 16.5+ engines).

The screenshot shows the Retrospect Management Console interface displaying a list of scripts. The left sidebar is the same as in the previous screenshot. The main area displays a table of scripts for 'Distributed Office' and 'Retrospect, Inc.' engines.

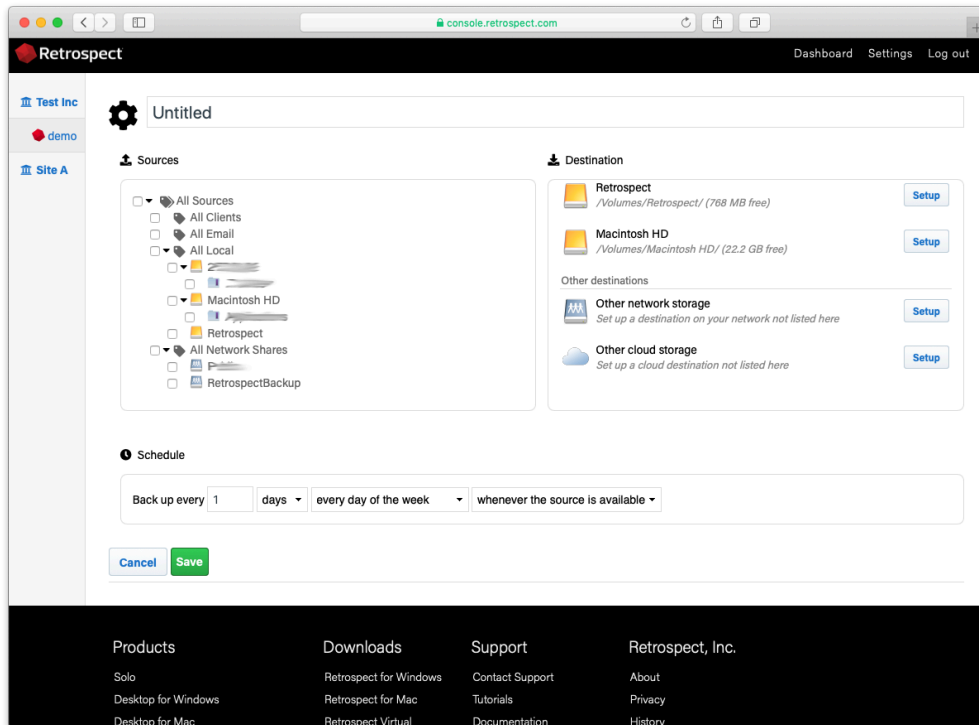
Name	Type	Source	Destination	Schedule	Modified
Distributed Office					
JG's MacBook Pro					
Copy Backups	Transfer Snapshots	Morgan's Email	Media Set A	unscheduled	8/29/2019, 12:38:24 PM
Daily Backup	ProactiveAI Backup	-	Media Set A	never	8/29/2019, 12:38:24 PM
Nufter test	Backup	Drобо Screenshots and 1 other	Media Set A	10:00 PM Every 0 weeks on Mon...	8/29/2019, 12:38:24 PM
Restore Test	Restore	Morgan's Email	Drобо Screenshots	unscheduled	8/29/2019, 12:38:24 PM
Retrospect, Inc.					
Andrew Dell Server					
Archive Files/Folders	Manual Archiving	-	-	unscheduled	9/24/2019, 4:45:04 PM
Backup Set Snapshot...	-	-	TransferTest	unscheduled	9/24/2019, 4:45:04 PM
Backup Set Transfer	Backup Set Transfer	-	-	unscheduled	9/24/2019, 4:45:05 PM
BATRegress_BUG_81...	Backup	BAT	BATS3_none_0-Administrator-192...	unscheduled	9/24/2019, 4:45:04 PM
Immediate Backup	Manual Backup	4MIFolders	IMAP	unscheduled	9/24/2019, 4:45:05 PM
Restore from Backup	Manual Restore	backup@retrospectinc.onmicro...	tsfRestore	unscheduled	9/24/2019, 4:45:04 PM
Searching and Retrieval	Manual Search	-	Local Disk (C:)	unscheduled	9/24/2019, 4:45:05 PM
Andrew's MacPro					
DrобоTransfer	Transfer Backup Sets	5GLocalBU	SGTransferDrобо	unscheduled	9/17/2019, 3:06:09 PM
ProScript	ProactiveAI Backup	Macintosh_HD 2 and 11 others	SGTransferDrобо	always	9/17/2019, 3:06:09 PM
Restore Assistant - 7/...	Restore	ubuntu17b6...	/	unscheduled	9/17/2019, 3:06:09 PM
Restore Assistant - 7/...	Restore	ubuntu17b6...	/	unscheduled	9/17/2019, 3:06:09 PM
Restore Assistant - 7/...	Restore	WIN-0883KRBAE96-C...	Local Disk (C:)	unscheduled	9/17/2019, 3:06:09 PM
SpeedTest	Backup	-	DebugLogTest	unscheduled	9/17/2019, 3:06:09 PM

Script Creation

Retrospect Management Console lets customers create and edit scripts for individual engines, and those changes are sent to each engine every minute. This includes the creation of destinations as well, including local disk sets, NAS disk sets, and cloud sets.

Select "Scripts" at the top.

Select "New Script" on the right.

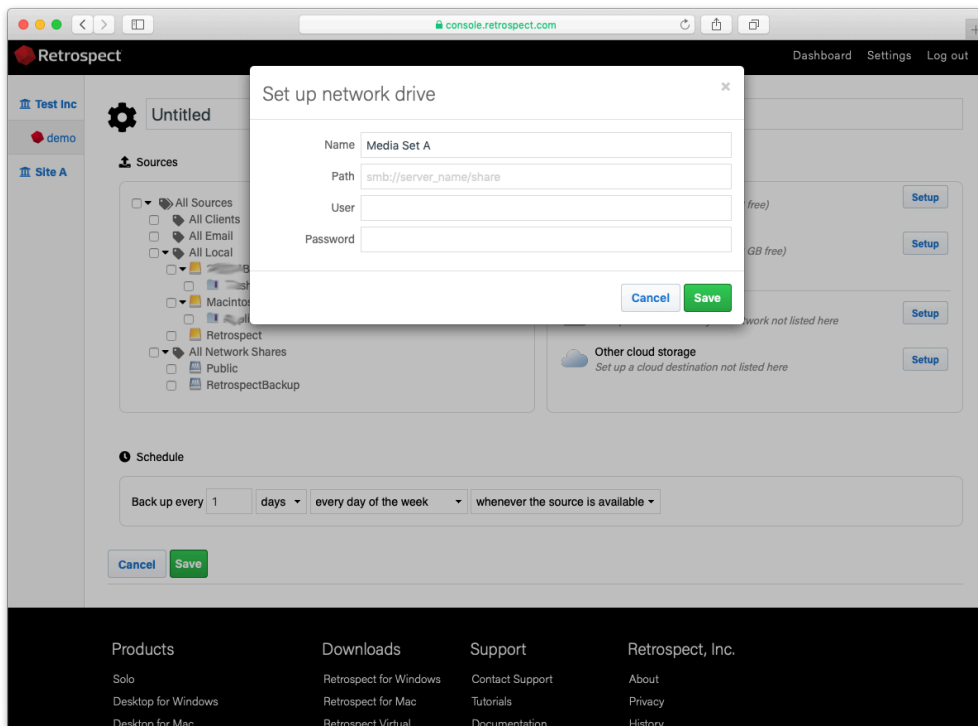


Type in a script name.

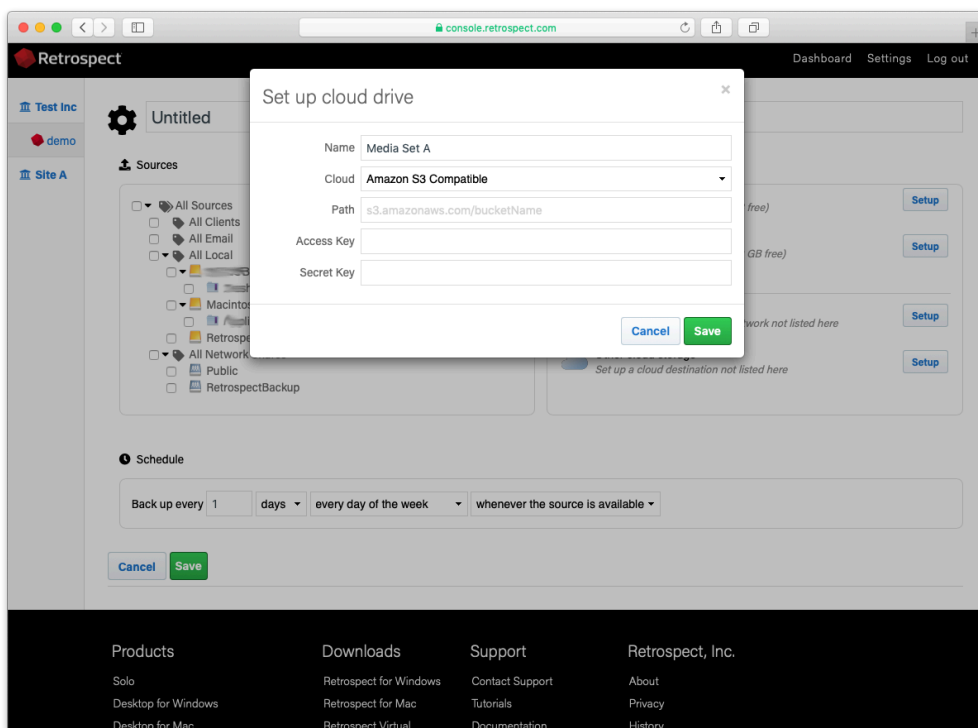
Select the sources to back up.

Select the destination to use. You can choose from existing "Backup Sets", existing destinations under "Available Drives" to create a new backup set on, and new destinations under "Other destinations" for a choice of new cloud storage or new NAS storage.

To set up a new NAS destination, select "Other network storage". You will see a popup where you can enter the name, path, user, and password for that NAS. Select "Save".



To set up a new cloud destination, select "Other cloud storage". You will see a popup where you can enter name, cloud (S3-compatible or Backblaze B2), path, access key, and secret key. Select "Save".



Select the appropriate schedule for the script.

Select "Save" to create the script. It will be synced to the engine in a couple minutes.

Shared Scripts

Log into your [Retrospect Management Console](#) account and click on "Settings" to access your account at the top right of the screen.

Click on "Scripts". You will see a list of Shared Scripts with a summary of each, including deployments.

Name	Sources	Destinations	Schedule	Deployed
Daily Backup	All email	B2 Backup	Every 2 days	17 deployments, 14 pending
Weekly Backup	All sources	S3 Backup-2	Every 7 days	17 deployments, 16 pending
Monthly Backup	All email	S3 Backup-2	Every 30 days	4 deployments, 4 pending

Click on "New Shared Script". You will be able to select which source containers you want to include, which cloud destination, and the schedule.

For the "Destination", you can select between Amazon S3 compatible providers and B2. For a B2 cloud destination, enter the bucket name. For an Amazon S3 compatible provider, use the entire URL with bucket name.

After you save the script, select that script's deployment options. Select the engines that you would like to deploy this Shared Script to and click "Save". The script will then be deployed to those engines.

Deployments for Daily Backup

Deploy the script to the following organizations and machines.

Script: [Daily Backup](#)
 Sources: All email
 Destination: B2 Backup
 Schedule: Every 2 days

[Cancel](#) [Save](#)

Name	Manage	Date Deployed	Security Code
<input checked="" type="checkbox"/> [Redacted Name]		1/8/2019, 1:11:47 PM
<input checked="" type="checkbox"/> [Redacted Name]		-
<input checked="" type="checkbox"/> [Redacted Name]		-
<input checked="" type="checkbox"/> [Redacted Name]		-
<input checked="" type="checkbox"/> [Redacted Name]		-
<input checked="" type="checkbox"/> [Redacted Name]		1/8/2019, 1:10:43 PM
<input checked="" type="checkbox"/> [Redacted Name]		-

All Shared Scripts are use AES-256 encryption. You will find the encryption key in the "Deployments" tab under "Security Code". Each backup set will be named 'Destination Name-Engine Name' to ensure the separate Storage Groups do not use the same destination path.

Compatibility

The latest versions of Retrospect Backup and Retrospect Virtual are compatible with Retrospect Management Console. See the following list for backwards compatibility. If your version is not listed, it is not compatible with Retrospect Management Console.

Retrospect Backup 15.5: Basic monitoring.

Retrospect Backup 16.0: Shared scripts.

Retrospect Backup 16.1: Management abilities with pause/unpause stop support.

Retrospect Backup 16.5: Remote granular management.

Retrospect Backup 17: Full compatibility.

Retrospect Virtual 2020: Monitoring compatibility via Automatic Onboarding.

Email Protection

Retrospect 15 for Windows and Mac are certified to back up and migrate most major email services that support IMAP. Follow these step-by-step instructions for configuring Retrospect.

Configuration

Retrospect needs the following pieces of information to access your email account:

Email Address – *your_email_address@example.com*

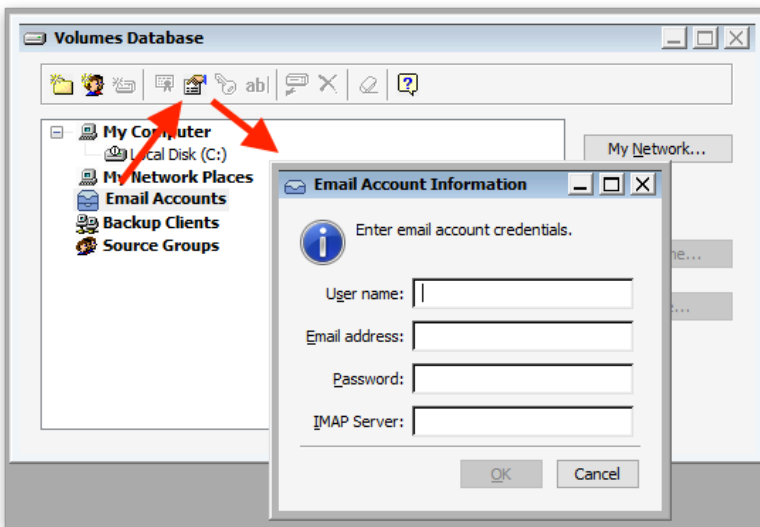
User Name – *your full name* (for display purposes only)

Password – *your email password*

IMAP Server – *your service's IMAP server name* (see your service's mail setup information for details)

IMAP Port – *993* (Mac only, Windows always set to *993*)

On Windows, select "Email Accounts" under "Volumes" and click "Properties" to add an email account.



On Mac, select the plus button under "Sources" and then "Email" to add an email account.

Script Clients Share Email Media Set Rule Server

Email Address:

User Name:

Password:

Use SSL

IMAP Server:

IMAP Port:

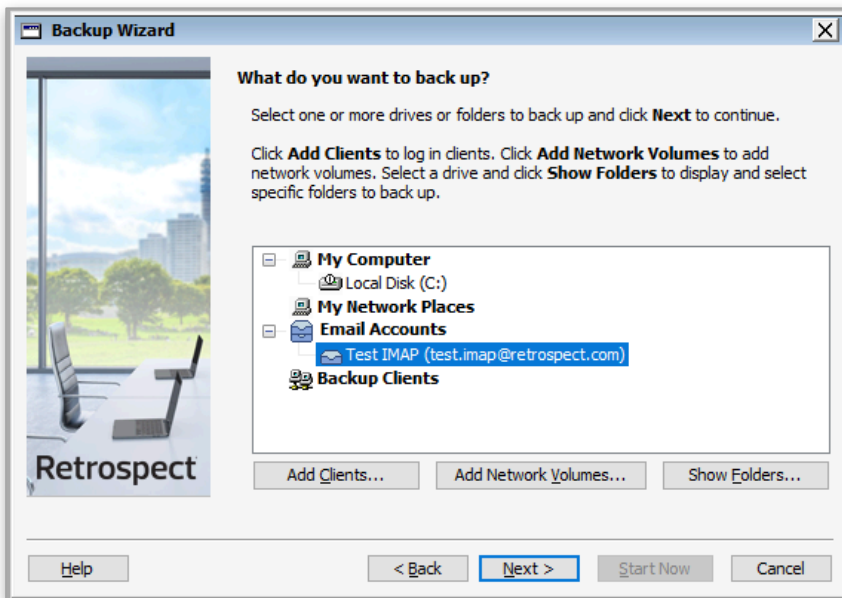
Cancel Add

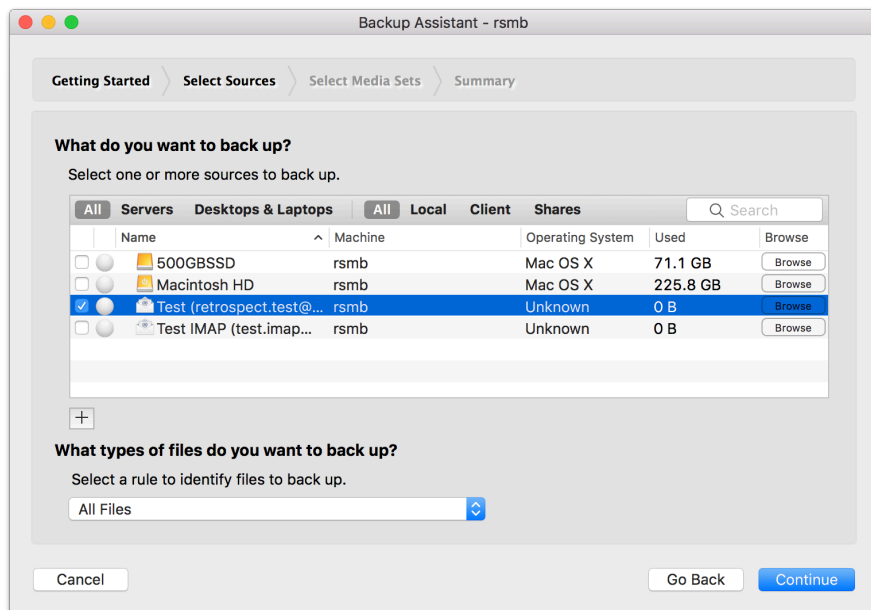
If you receive "error 8256", please check your email address and password.

If you receive "error 8252", please check your IMAP server and port.

Adding Email Account to Backup Script

Adding an email account to a backup script is the same as any other source. Launch the Mac Backup Assistant or Windows Backup Wizard and select the email account as a source. If you use the advanced mode, the email accounts are listed along with the other sources.





Performance

Below are performance metrics for gauging how long your email operations will take. Keep in mind that they vary greatly by the email service's responsiveness.

Scanning: For scanning, Retrospect downloads successive sets of email headers. We have seen Retrospect scan 150 emails per second for 100,000 emails on a Gmail account, taking 10 minutes. We have also seen instances where scan is as slow as 10 emails per second.

Backup: For backup, Retrospect downloads each email in serial. In testing, we have seen a backup of 30,000 emails with 3 GB of data take 2.5 hours, averaging 3 Mbps. However, similar to scanning variance, we have seen backups that were far slower.

Throttling: All major email providers use throttling to control their bandwidth usage. It does not affect normal email usage or small backups and restores, but for large backups and restores, you will likely encounter throttling. Here are a couple examples: [Gmail bandwidth limits](#) and [Office 365 limits](#). For an overall view, Office 365 provides [estimates for how long large migrations take](#).

Remote Data Protection

VPN Backup

Optimized for remote employees on VPN that you want to protect with an on-site Retrospect Backup instance.

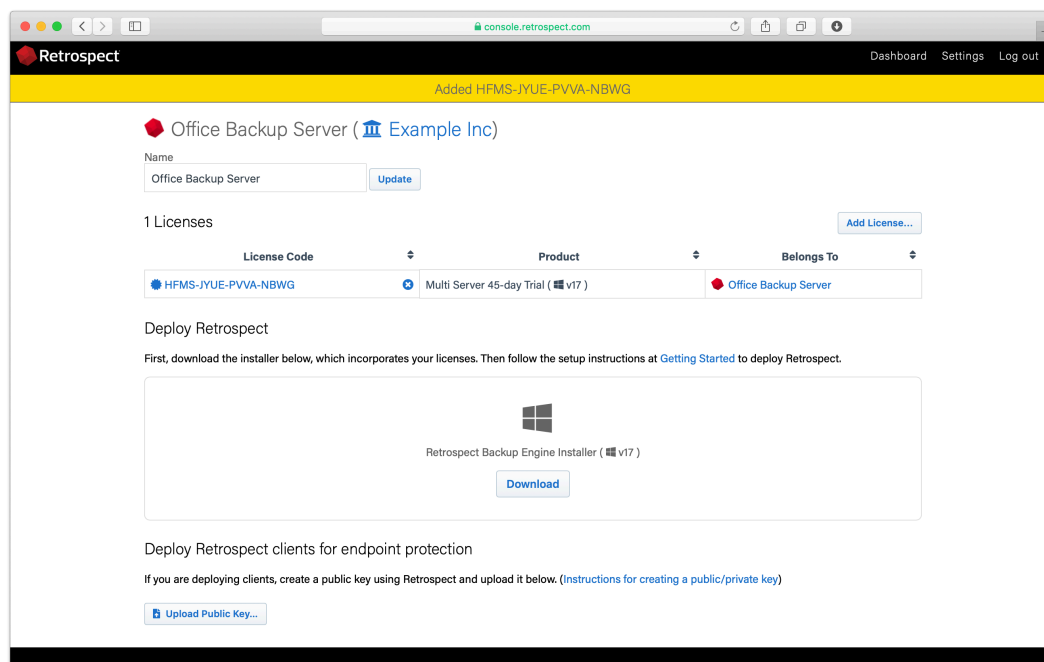
Retrospect Backup works seamlessly with VPNs. If your VPN supports multicast, Retrospect Backup will automatically discover and protect servers and endpoints that are connected over the VPN. If multicast is not supported, you can add servers, desktops, and laptops by their IP address. You can quickly onboard new remote employees using Automatic Onboarding on Retrospect Management Console.

Let's walk through the steps with Automatic Onboarding on Retrospect Management Console.

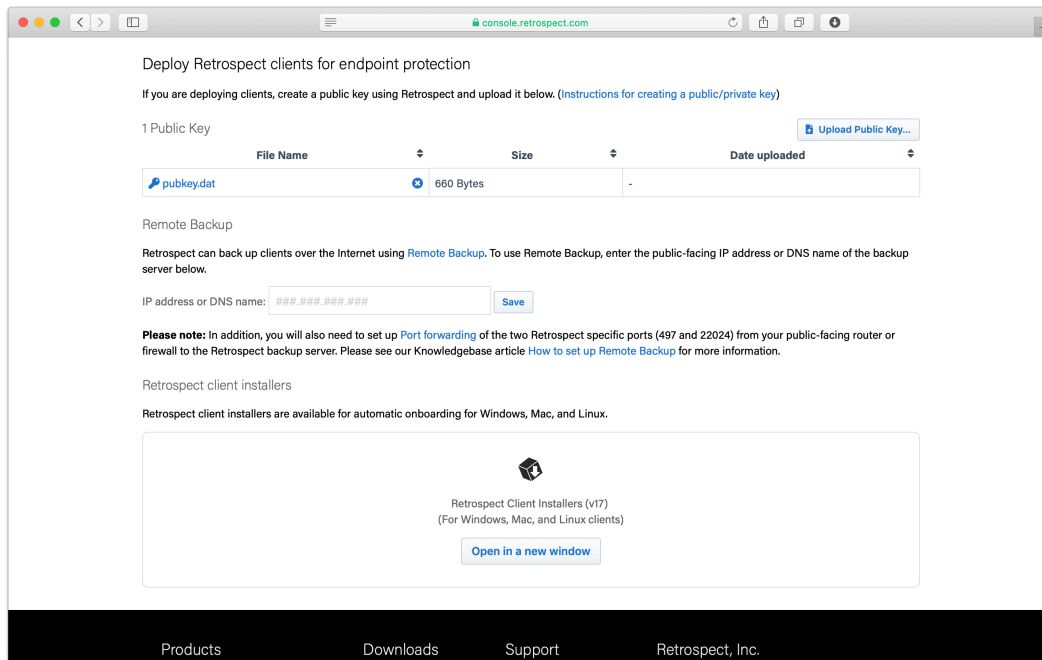
Retrospect Backup for Windows: Onboard a new server or endpoint

Retrospect Backup for Mac: Onboard a new server or endpoint

In the backup server's page, scroll down to see "Deploy Retrospect clients for endpoint protection". Note that servers are supported now as well.

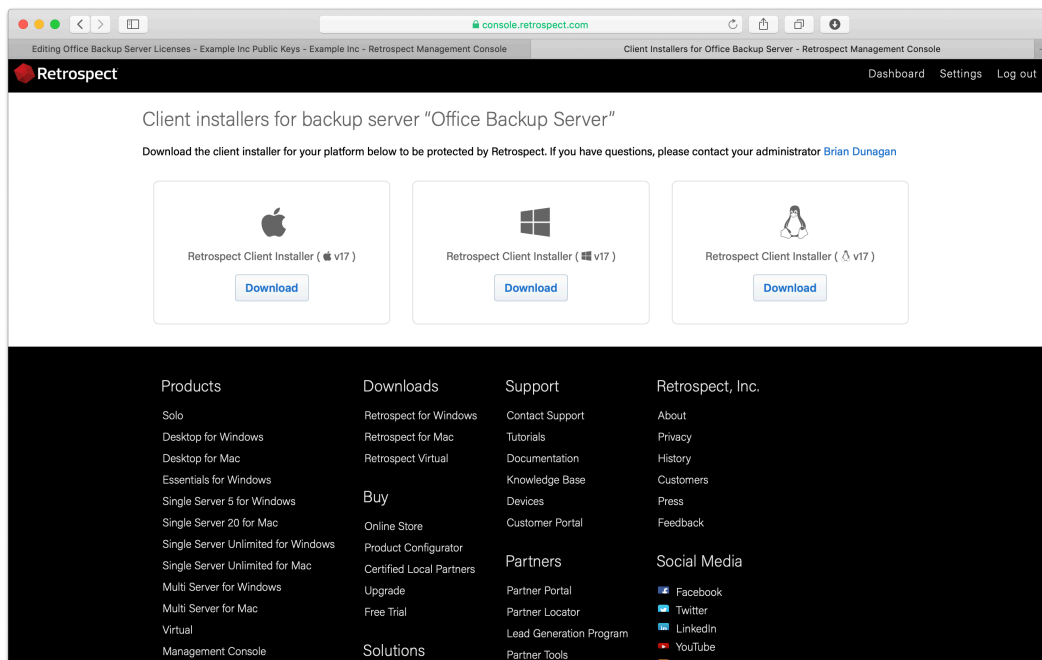


Upload the server's public key. Retrospect Backup 17 enables you to automatically upload it to Retrospect Management Console. Simply go to Preferences. The public key file is located on the engine under `/Library/Application Support/Retrospect/pubkey.dat` on Mac and `C:/ProgramData/Retrospect/pubkey.dat` on Windows. Find it with "Upload Key" and then click "Upload".



+

Under "Retrospect client installers", there is a link to share with end users. They can download the Retrospect Client for Windows, Retrospect Client for Mac, or Retrospect Client for Linux installers with the public key and remote backup address bundled in.



Your Retrospect Client agents are now set up to connect to your Retrospect Backup instance. Now we need to set up the Retrospect Backup instance to automatically add them and protect them.

Let's walk through setting these up in Retrospect Backup without Retrospect Management Console.

Under Preferences > Clients, create a public/private keypair.

Locate the public key file.

Copy the public key file into the Retrospect Client installer's "public_key" folder. You can download the Retrospect Client installer from [Retrospect Downloads](#).

Compress the new installer and send it to your remote employee to install.

Now that the Retrospect Client agent can connect to the Retrospect Backup instance, let's create a ProactiveAI backup script.

In Retrospect Backup, go to Preference then Clients and check "Automatically add clients using public keys".

Create a ProactiveAI script. This is under ProactiveAI on Windows and under Scripts on Mac.

Add a backup set as a destination. This can be either local storage or a cloud storage location.

Add "Automatically Added Clients" as the source. This is under Volumes on Windows and under Tags on Mac.

After you save, Remote Backup will be configured.

If you encounter any issues, please see further details in our User's Guide: [Retrospect Backup for Windows](#) or [Retrospect Backup for Mac](#).

Remote Backup

Optimized for remote employees outside of VPN that you want to protect with an on-site Retrospect Backup instance.

With Remote Backup, remote employee endpoints can be automatically added to a Retrospect Backup instance inside the corporate firewall and protected with a ProactiveAI script. There are no router changes needed on the employees side, and the IT administrator can make a simple change on the corporate firewall to forward inbound connections to Retrospect Backup. Remote employees are able to use on-demand restore to get files fast without assistance. Automatic Onboarding is a great way to deploy the Retrospect Client agent to your remote employees.

Remote Backup is designed specifically for endpoint protection and is not supported for server protection.

For Remote Backup to work, the Retrospect Client agent needs to be able to make a network connection the Retrospect Backup instance.

Enable port forwarding for two ports to forward from the server-side public-facing IP on the router/ NAT/firewall to the Retrospect engine.

Set up the Retrospect engine to accept remote backups.

Set up the Retrospect client to send periodic backup requests to the engine.

We'll walk through each step.

Server-Side Network Configuration

Port Forwarding is a standard mechanism to redirect connections on a specific port from one IP to another. Retrospect Backup requires two ports:

Port 497: multicast and remote backup broadcast

Port 22024: on-demand requests

You need to set up your public-facing router/NAT/firewall to forward these ports to the IP address of the computer running your Retrospect Backup instance. With this networking change, a remote endpoint running the Retrospect Client agent will be able to make a connection to the Retrospect Backup instance, even though the computer running the Retrospect Backup instance is running on the internal network.

For guidance on enabling port forwarding, please refer to the hardware's manual. The process varies by manufacturer.

You can verify that the ports are open using <https://www.yougetsignal.com/tools/open-ports/>. Remote backup will not work unless the ports are open.

Retrospect Backup Configuration

Retrospect Backup utilizes the following features for Remote Backup:

Public/Private Keypair Authentication: This authentication automatically and securely identifies the remote endpoint as a trusted client without a password.

ProactiveAI Backup: This backup script will automatically starts a backup for any remote endpoint that notifies the Retrospect Backup instance of its availability.

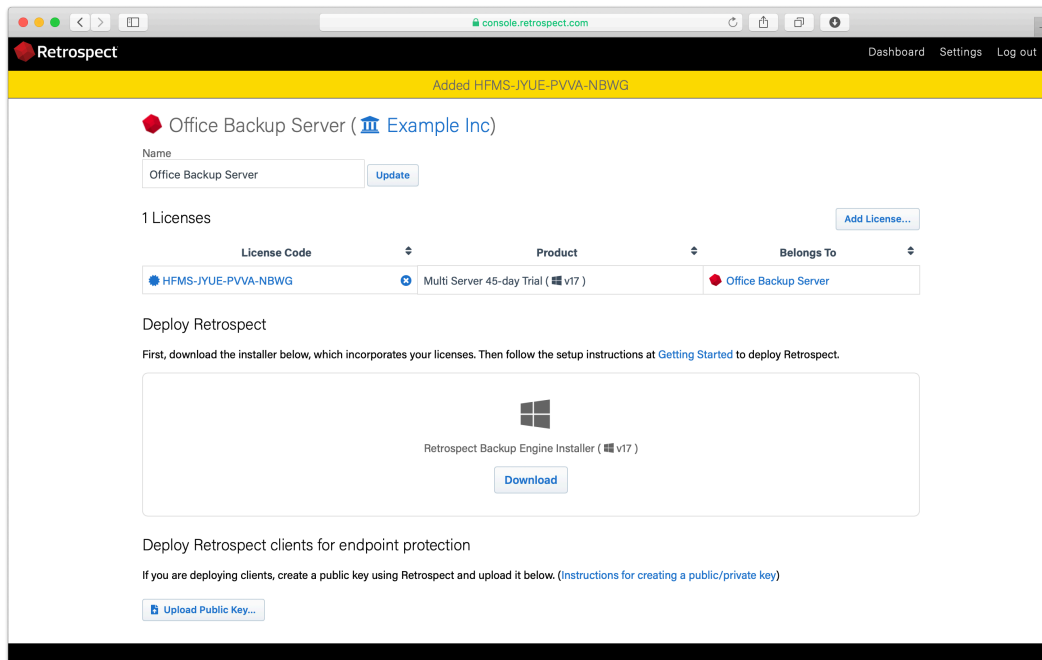
On-Demand Restore: This restore workflow allows remote employees to restore files themselves without IT assistance.

Let's walk through the steps with Automatic Onboarding on Retrospect Management Console.

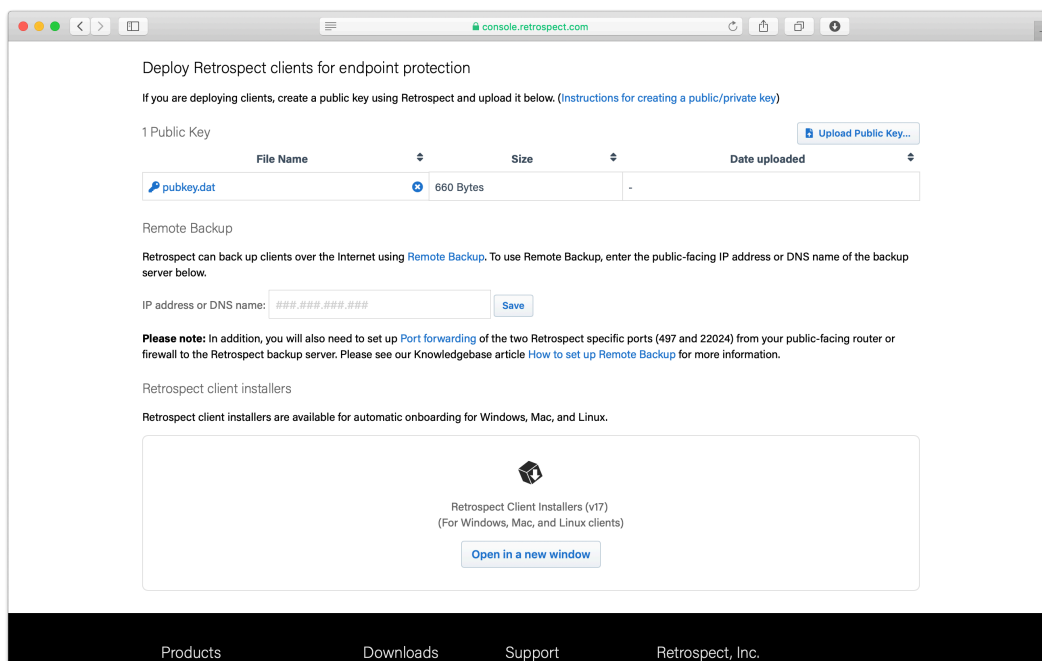
Retrospect Backup for Windows: Onboard a new server or endpoint

Retrospect Backup for Mac: Onboard a new server or endpoint

In the backup server's page, scroll down to see "Deploy Retrospect clients for endpoint protection".



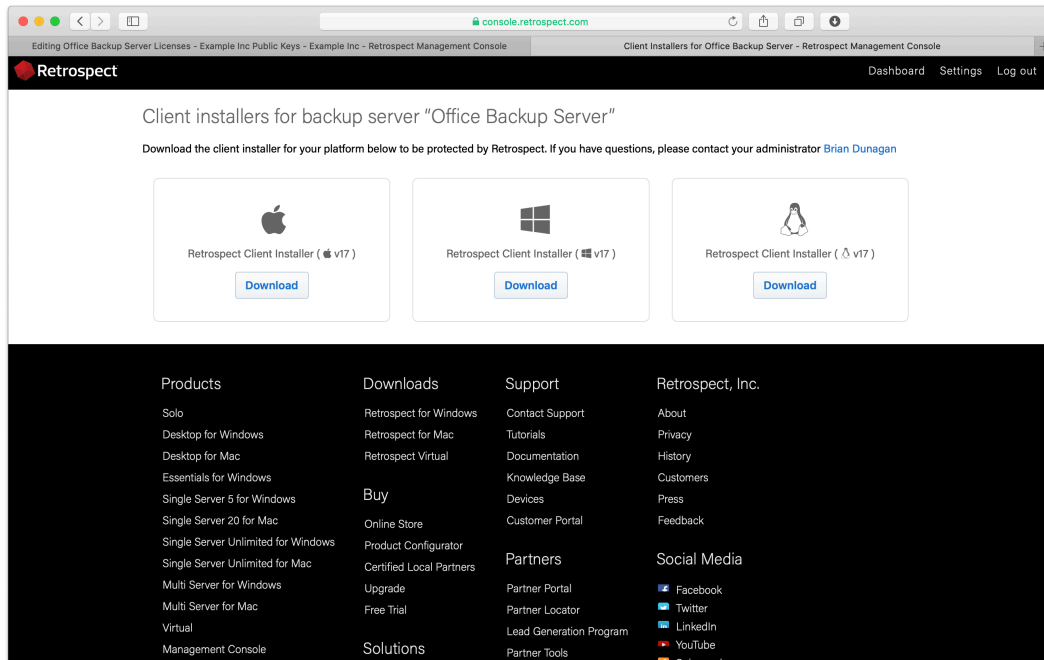
Upload the server's public key. Retrospect Backup 17 enables you to automatically upload it to Retrospect Management Console. Simply go to Preferences. The public key file is located on the engine under `/Library/Application Support/Retrospect/pubkey.dat` on Mac and `C:/ProgramData/Retrospect/pubkey.dat` on Windows. Find it with "Upload Key" and then click "Upload".



Enter the IP address or DNS name of the Retrospect Backup server under "Remote Backup", so that remote computers can connect to the port-forwarded public IP/DNS address.

Under "Retrospect client installers", there is a link to share with end users. They can download the Retrospect Client for Windows, Retrospect Client for Mac, or Retrospect Client for Linux installers

with the public key and remote backup address bundled in.



Let's walk through setting these up in Retrospect Backup without Retrospect Management Console.

Under Preferences > Clients, create a public/private keypair.

Locate the public key file.

Copy the public key file into the Retrospect Client installer's "public_key" folder. You can download the Retrospect Client installer from [Retrospect Downloads](#).

Create a file called "server.txt" in the following location with the public DNS/IP address of the Retrospect Backup instance.

Win: In the same folder as Retrospect Client MSI file.
Mac: In the same folder as "Retrospect Client Installer".

```
Sample `server.txt` File  
backup.example.com
```

Compress the new installer and send it to your remote employee to install.

Now that the Retrospect Client agent can connect to the Retrospect Backup instance, let's create a ProactiveAI backup script.

In Retrospect Backup, go to Preference then Clients and check "Automatically add clients using public keys".

Create a ProactiveAI script. This is under ProactiveAI on Windows and under Scripts on Mac.

Add a backup set as a destination. This can be either local storage or a cloud storage location.

Add "Remote Backup Clients" as the source. This is under Volumes on Windows and under Tags on

Mac.

After you save, Remote Backup will be configured.

On-demand restore will automatically work using public key authentication.

If you encounter any issues, please see further details in our User's Guide: [Retrospect Backup for Windows](#) or [Retrospect Backup for Mac](#).

Cloud Backup

Optimized for remote employees that you want to bypass corporate network and back up to the cloud.

With Cloud Backup, remote employees can use Retrospect Backup to back up their corporate data to a cloud storage provider. Retrospect Management Console supports Automatic Onboarding to deliver a Retrospect Backup download and license to remote employees, and IT administrators can then configure a Shared Script on Retrospect Management Console to automatically deploy to those new instances. The endpoint will use the script to back itself up to a per-configured cloud storage location. Retrospect Backup Solo Premium is a great subscription license for this scenario, covers a computer and any connected device.

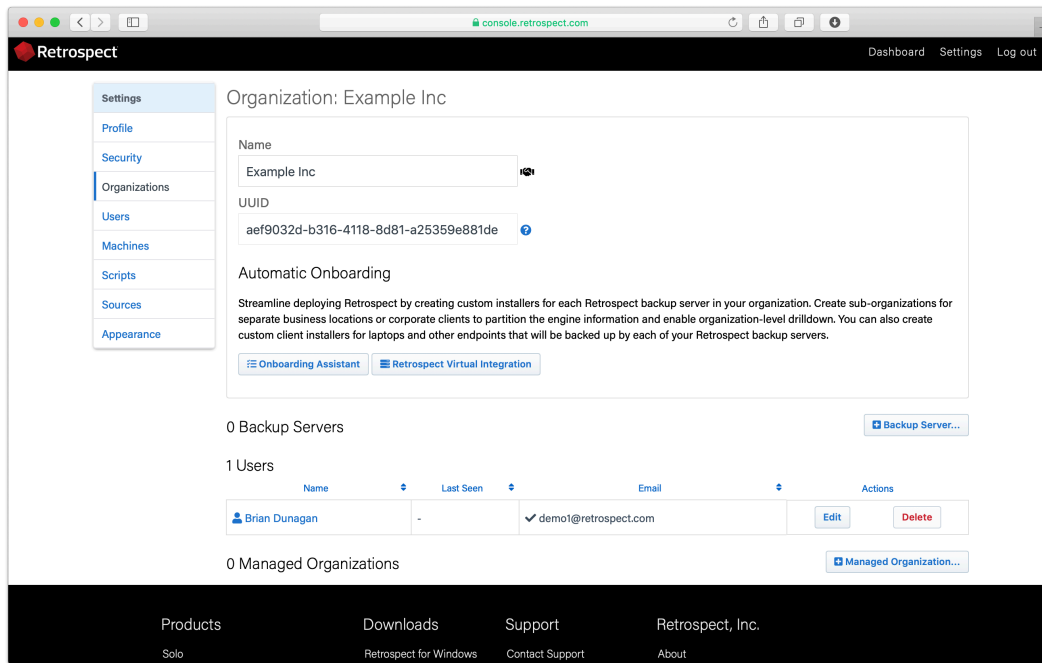
Let's walk through setting up a new Retrospect Backup server and then using Shared Scripts to deploy a cloud backup script to it.

Automatic Onboarding

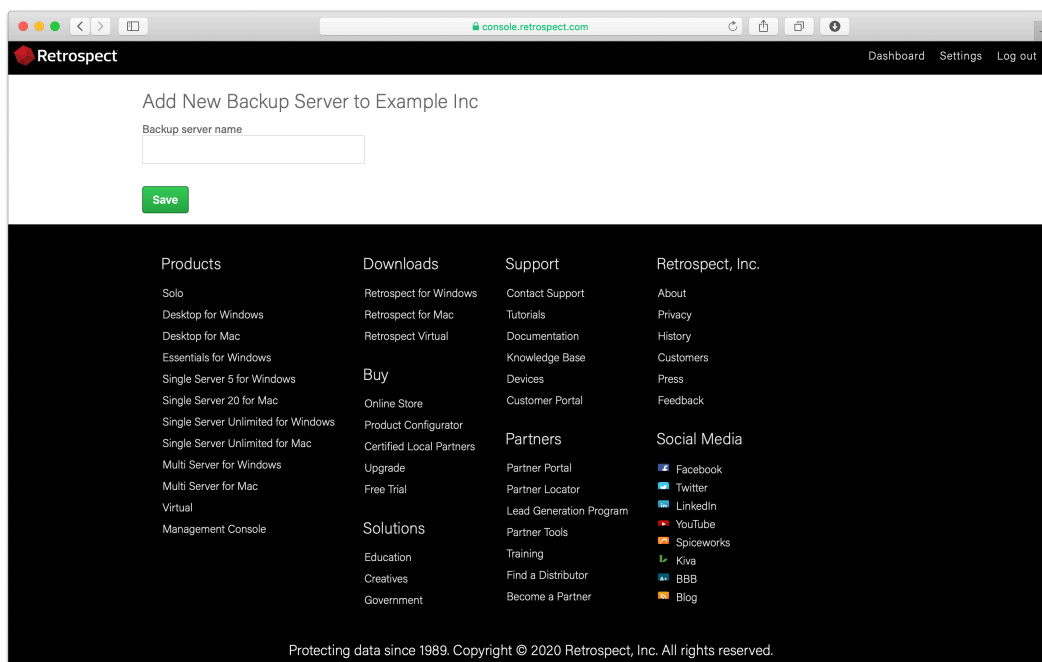
Retrospect Backup for Windows: Onboard a new backup server

Retrospect Backup for Mac: Onboard a new backup server

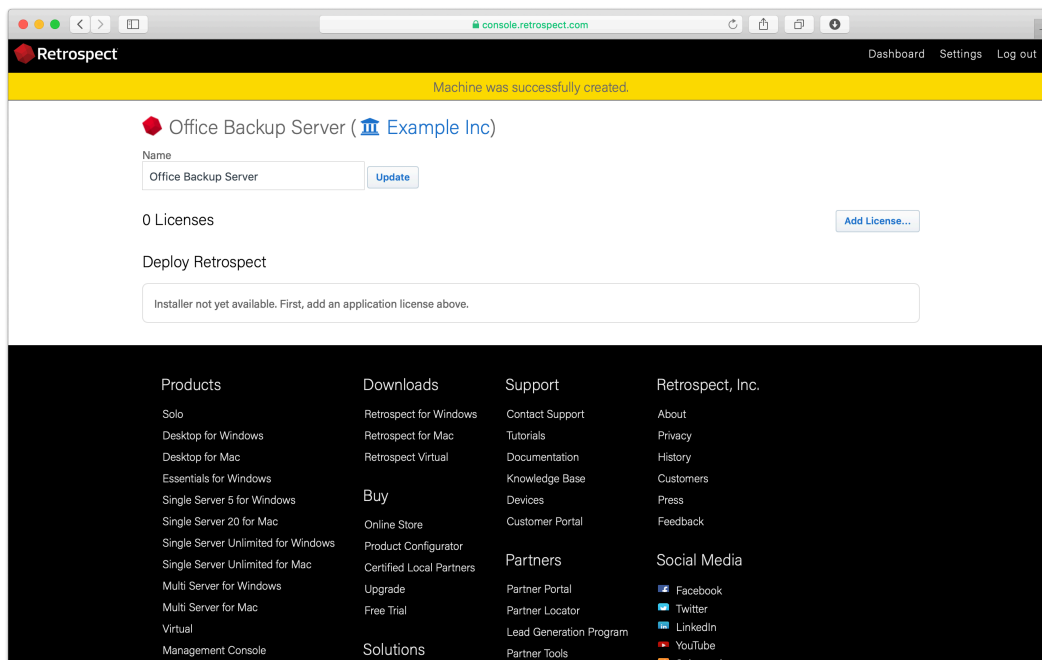
Under Settings > Organizations, you will see our new Onboarding Assistant. Click "Onboarding Assistant".



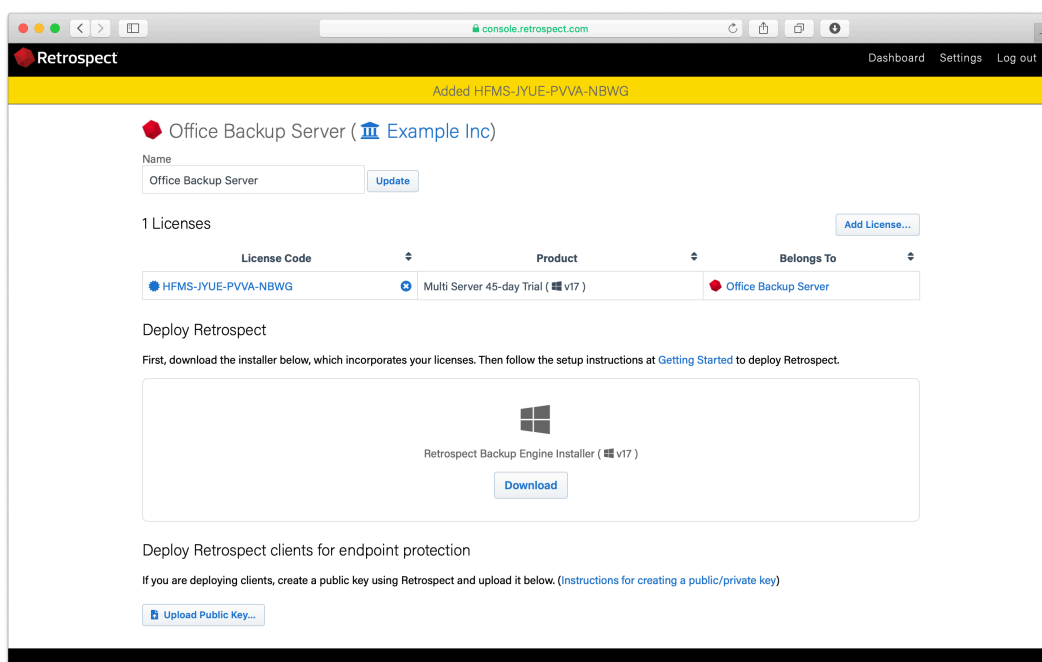
Enter a name for your new backup server.



Click "Add License...", type in your license, and click "Add".



Your custom installer should now be visible. Click "Download".



Unzip the download.

For Mac, run "Install Retrospect". At the end, Retrospect will be launched.

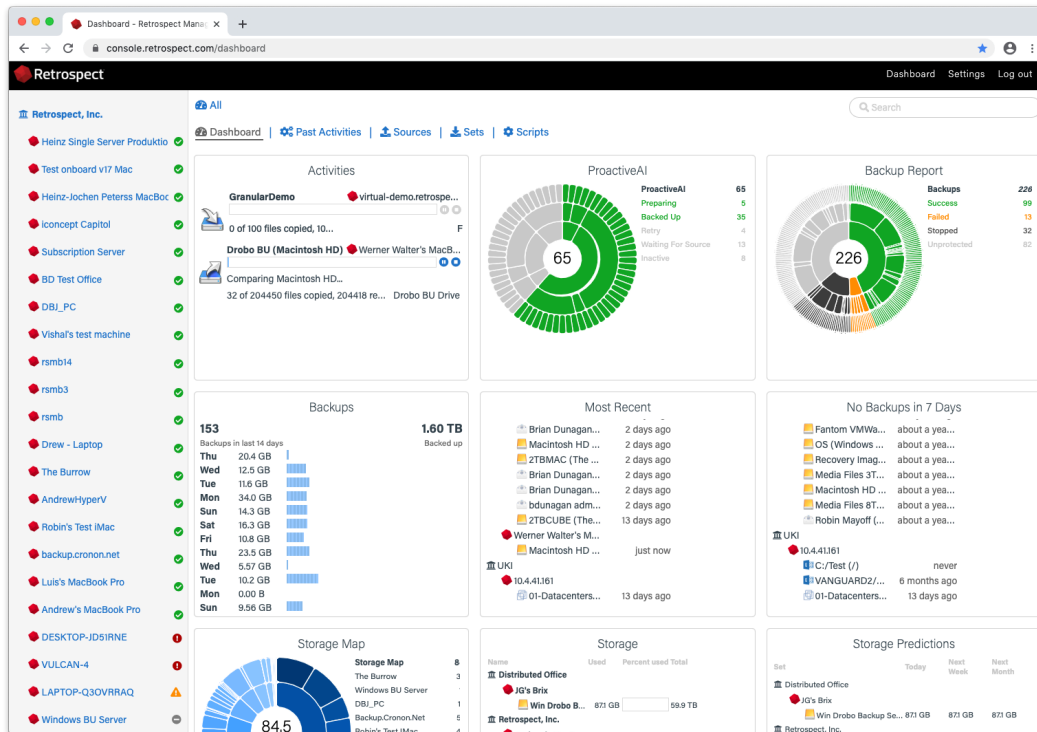
For Windows, run "Install Retrospect" and select "Install Retrospect". After it completes, launch Retrospect.

Retrospect is now licensed and connected to Retrospect Management Console under your account.

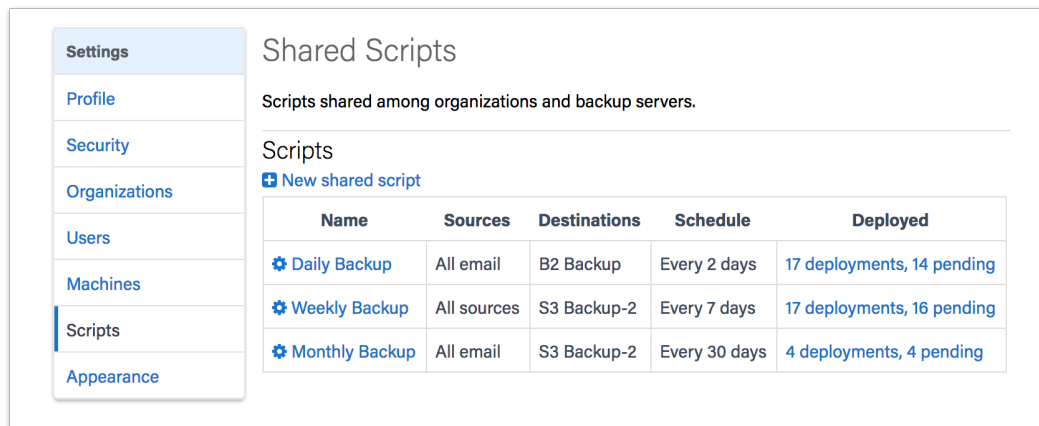
Deploying a Shared Script

The Retrospect Management Console supports mass deployment of scripts through its Shared Scripts workflow. With Shared Scripts, IT administrators or partners can update a set of Retrospect Backup engines with a common ProactiveAI script to a single cloud destination. See the following step-by-step guide.

Log into your [Retrospect Management Console](#) account and click on "Settings" to access your account at the top right of the screen.



Click on "Scripts". You will see a list of Shared Scripts with a summary of each, including deployments.



Click on "New Shared Script". You will be able to select which source containers you want to include, which cloud destination, and the schedule.

Settings

- Profile
- Security
- Organizations
- Users
- Machines
- Scripts
- Appearance

Edit Daily Backup

Daily Backup

Sources

- All sources
- All local
- All clients
- All network
- All email

Destination

B2 Backup [Edit](#)

Schedule

Backup every 1 days

Options

Verification: Thorough Verification

- Data Compression
- Block Level Incremental Backup

[Cancel](#) [Save](#) [Delete](#)

For the "Destination", you can select between Amazon S3 compatible providers and B2. For a B2 cloud destination, enter the bucket name. For an Amazon S3 compatible provider, use the entire URL with bucket name.

Destination

B2 Backup

Name: B2 Backup

Type: Backblaze B2

Path: bucketname

ID: [Redacted]

Secret: [Redacted]

Cancel Save

After you save the script, select that script's deployment options. Select the engines that you would like to deploy this Shared Script to and click "Save". The script will then be deployed to those engines.

Settings | Profile | Security | Organizations | Users | Machines | Scripts | Appearance

Deployments for Daily Backup

Deploy the script to the following organizations and machines.

Script: [Daily Backup](#)
 Sources: All email
 Destination: B2 Backup
 Schedule: Every 2 days

Cancel Save

Name	Manage	Date Deployed	Security Code
[Redacted]	[Edit]	1/8/2019, 1:11:47 PM	[Redacted]
[Redacted]	[Edit]	-	[Redacted]
[Redacted]	[Edit]	-	[Redacted]
[Redacted]	[Edit]	-	[Redacted]
[Redacted]	[Edit]	-	[Redacted]
[Redacted]	[Edit]	1/8/2019, 1:10:43 PM	[Redacted]
[Redacted]	[Edit]	-	[Redacted]

All Shared Scripts are use AES-256 encryption. You will find the encryption key in the "Deployments" tab under "Security Code". Each backup set will be named 'Destination Name-Engine Name' to ensure the separate Storage Groups do not use the same destination path.

Block Level Incremental Backup

Overview

Retrospect now has the ability to back up only the parts of a file that have changed. Many applications like Microsoft Outlook for Windows and FileMaker have large files that are constantly changing by small increments. After you enable block level incremental backup for a backup script, the next backup will be a full backup of modified files. For large files, subsequent backups using that backup script will be incremental, storing only blocks that changed since the prior backup. When restoring a file backed up using this feature, Retrospect first restores the full backup and then the subsequent increments. To restore the 5th backup of a file, for example, Retrospect will restore that file's first full backup, and then each of the next four increments of that file.

Block level incremental backup works with existing Retrospect file level features. If a backup uses a selector/rule, only selected files are backed up fully or incrementally. If matching is enabled, any file that has a matching version in the backup set is skipped entirely. If software compression is enabled, block level increments are compressed and then stored in the backup set. When transferring snapshots or backup sets containing block level incremental backups of a file, the complete chain of prior increments leading to and including the full version of that file is automatically transferred. During grooming, if an increment of a file is preserved based on the grooming policy, the complete chain of prior increments leading to and including the full version of that file is automatically preserved.

Block level incremental backup works with various backup set types, such as disk, file and tape.

Storage Savings

With block level incremental backup enabled, significant storage savings is possible when backing up certain large files, above 90% for daily use in some cases.

Application	File Type	Use	Savings
Microsoft Outlook 2013 for Windows	.pst	Daily use with 100 new emails	95%
Microsoft Outlook 2011 for Mac	Database	Daily use with 100 new emails	93%
Microsoft Entourage 2008 for Mac	n/a	Daily use with 100 new emails	95%
Microsoft Exchange 2013	.edb	Daily use	90%

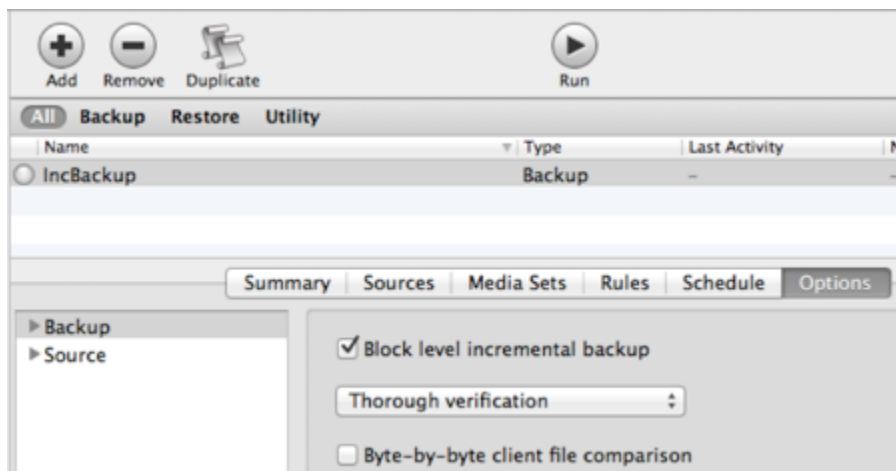
Application	File Type	Use	Savings
FileMaker Pro 13	.fmp12	Add 20 records	85%
VMware Fusion 5 for Mac	.vmdk	Install 100 Windows Updates	60%
VMware Fusion 5 for Mac	.vmdk	Install Office then VM snapshot	70%

Depending on how a specific application stores and modifies its data, storage savings from block level incremental backup can vary. Retrospect automatically excludes a number of known file types that do not benefit from block level incremental backup, and you can add others easily. Find out more in [Options](#).

Usage

Block level incremental backup is a script and wizard option, available for use with all backup/media set types. The feature is off by default. You can enable it or disable it anytime. Once you enable block level incremental backup, the first backup will be a full backup of each new or modified file. During subsequent backups, only changed blocks are backed up for applicable files. Find out more in [Technical Details](#).

The option is available under Options in Backup, Archive, and Proactive scripts.



Applicable files

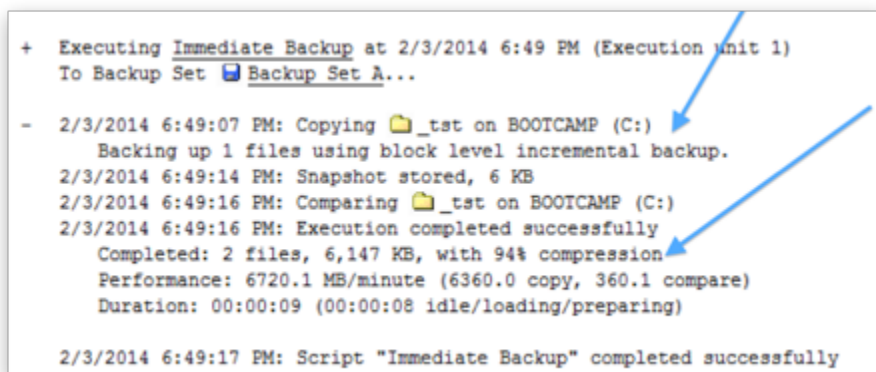
With block level incremental backup enabled, by default files 100 MB or larger will be backed up incrementally. Smaller files will automatically be backed up in full because restore overhead outweighs the benefits of incremental backup. Find out more in [Options](#)

For digital media files, some media authoring apps change the files substantially even when only small edits are made. In these cases, benefits from block level incremental backup will be limited.

Logging

While a backup is in progress, Retrospect shows the full size of the files being backed up. Once completed, Retrospect will show the size of the increments that are actually backed up.

The following example shows the Operations Log of a completed backup of two modified files. One of the files has a full size of 100 MB, of which 5 MB has changed since previous backup. The other file is 1 MB in size, not meeting the default criteria of block level incremental backup and therefore backed up in full. The resulting backup's actual size is about 6 MB (6,147 KB). Since this backup has software compression turned off, the 94% compression figure in the log indicates block level incremental backup has reduced the backup's size by 94%.



```
+ Executing Immediate Backup at 2/3/2014 6:49 PM (Execution unit 1)
  To Backup Set Backup Set A...

- 2/3/2014 6:49:07 PM: Copying _tst on BOOTCAMP (C:)
  Backing up 1 files using block level incremental backup.
2/3/2014 6:49:14 PM: Snapshot stored, 6 KB
2/3/2014 6:49:16 PM: Comparing _tst on BOOTCAMP (C:)
2/3/2014 6:49:16 PM: Execution completed successfully
  Completed: 2 files, 6,147 KB, with 94% compression
  Performance: 6720.1 MB/minute (6360.0 copy, 360.1 compare)
  Duration: 00:00:09 (00:00:08 idle/loading/preparing)

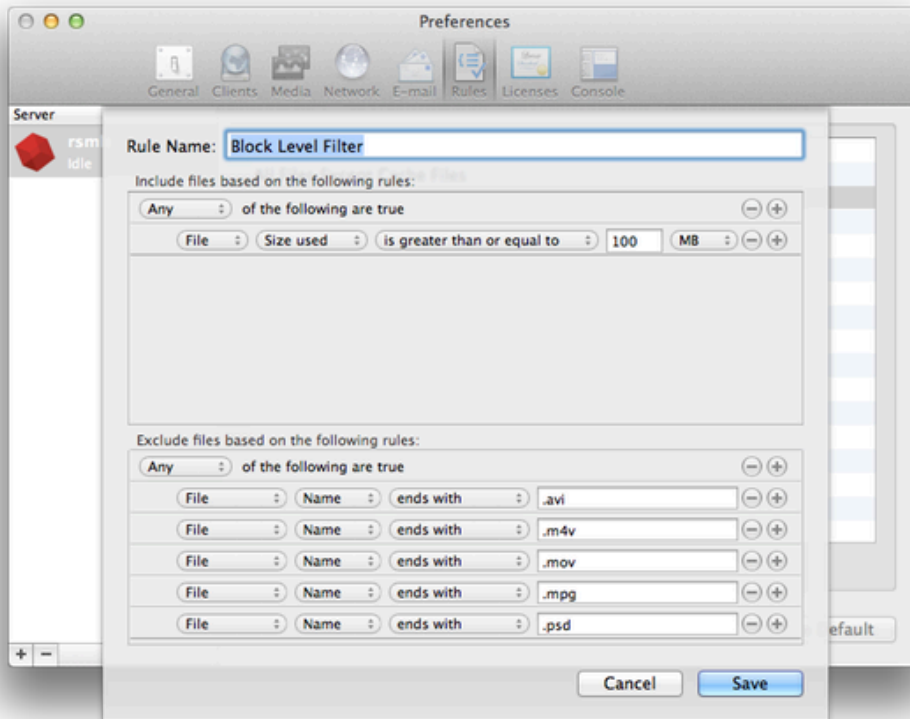
2/3/2014 6:49:17 PM: Script "Immediate Backup" completed successfully
```

When block level incremental backup is enabled, the amount of data shown in the progress panel can differ from the amount of data listed in the Operations Log. Retrospect calculates the data to be backed up based on the size of the files; however, the final number in the log is based on how much data was backed up. This final size varies according to how much was saved both via block level incremental backup as well as software compression.

Options

With block level incremental backup enabled, files 100 MB or larger will be backed up incrementally by default. Smaller files will automatically be backed up in full because restore overhead outweighs the benefits of incremental backup. This is customizable via a rule-selector named Block Level Filter. It controls how a file is backed up, i.e. whether it is backed up in full or incrementally. To select what files to back up, choose one of the other rules/selectors instead for your backup scripts, such as All Files Except Cache Files or User Files and Settings.

The Block Level Filter is in Preferences > Rules:



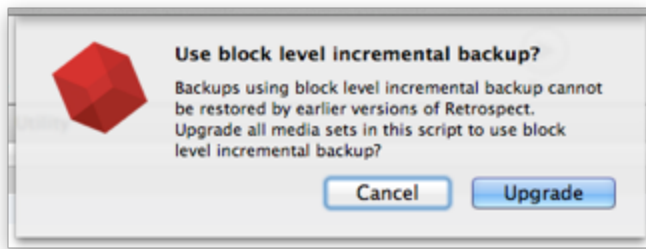
Other Thresholds

Block level incremental backup has two other thresholds: the number of backups and the number of days since prior backup. To reduce the risk of storage media loss breaking a chain of incremental backups (making some of the backups not restorable), Retrospect automatically performs a full backup if a file's 30 recent backups are all incremental, or if its most recent backup is more than 31 days old. These settings are customizable in `retro.ini`:

```
# retro.ini
[Options]
MaxFileBlockLevelBackups=30
NumDaysAllowedSinceLastBlockLevelBackup=31
```

Backward Compatibility

Block level incremental backups cannot be restored by earlier versions of Retrospect. When enabling a backup script for block level incremental backup, you will be prompted to upgrade the associated backup sets if they were created by a prior version of Retrospect. To keep the backup set compatible with prior Retrospect versions, cancel the upgrade prompt, and block level incremental backup will remain disabled.



Technical Details

Speed and size of a block level incremental backup depend on how a specific application stores and modifies its data. Applications like Apple Mail save each item—an email or a document—as a separate file. When these small files change, Retrospect can backup the whole file up quickly. Other applications store many items, database or disk image in a large file, so block level incremental backup should improve backup performance for these the most. For items like movies, photos, and music, the files themselves don't change, unless you edit them; Retrospect's standard backup with the matching feature will suffice.

After you enable block level incremental backup for a backup script, the next backup will be a full backup of new or modified files. During subsequent backups, each 2MB-block of applicable files is compared to its checksum from prior backup, and only changed blocks are backed up. For files not applicable to block level incremental backup, they will be backed up in full.

Instant Scan Technology

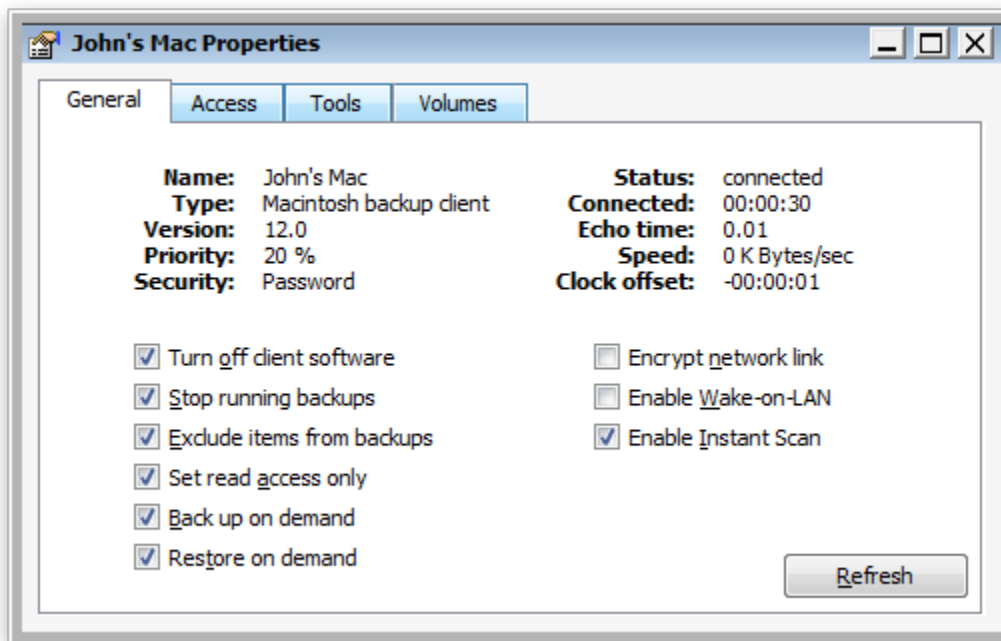
Retrospect now pre-scans NTFS and HFS+ volumes connected to the backup server and Retrospect clients, speeding overall backup and restore operations by removing the lengthy volume scan from backup process. This feature employs the USN change journal (for NTFS volumes) and FSEvents (for HFS+ volumes) to predetermine which files have changed since the last backup to a particular Media Set.

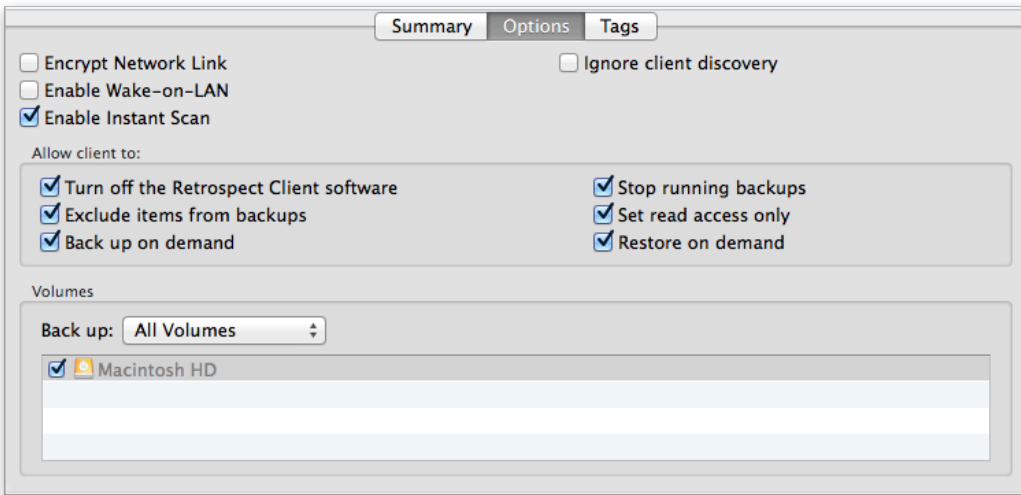
Instant Scan runs on the backup source computer. When Instant Scan data is used, the activity's execution log will show "Using Instant Scan." Starting from Retrospect 8.1.0 (266) for Windows and Retrospect 10.1.0 (221) for Mac, Instant Scan is only used for scheduled script activity, and not any activity manually started by clicking a Run button.

Enable or Disable Instant Scan

Retrospect Backup 10 for Windows / Retrospect Backup 12 for Mac

Instant Scan Centralized Management – In addition to client-side management, admins can now manage the state of Instant Scan in their environment through the server interface. You can enable or disable the feature per client.

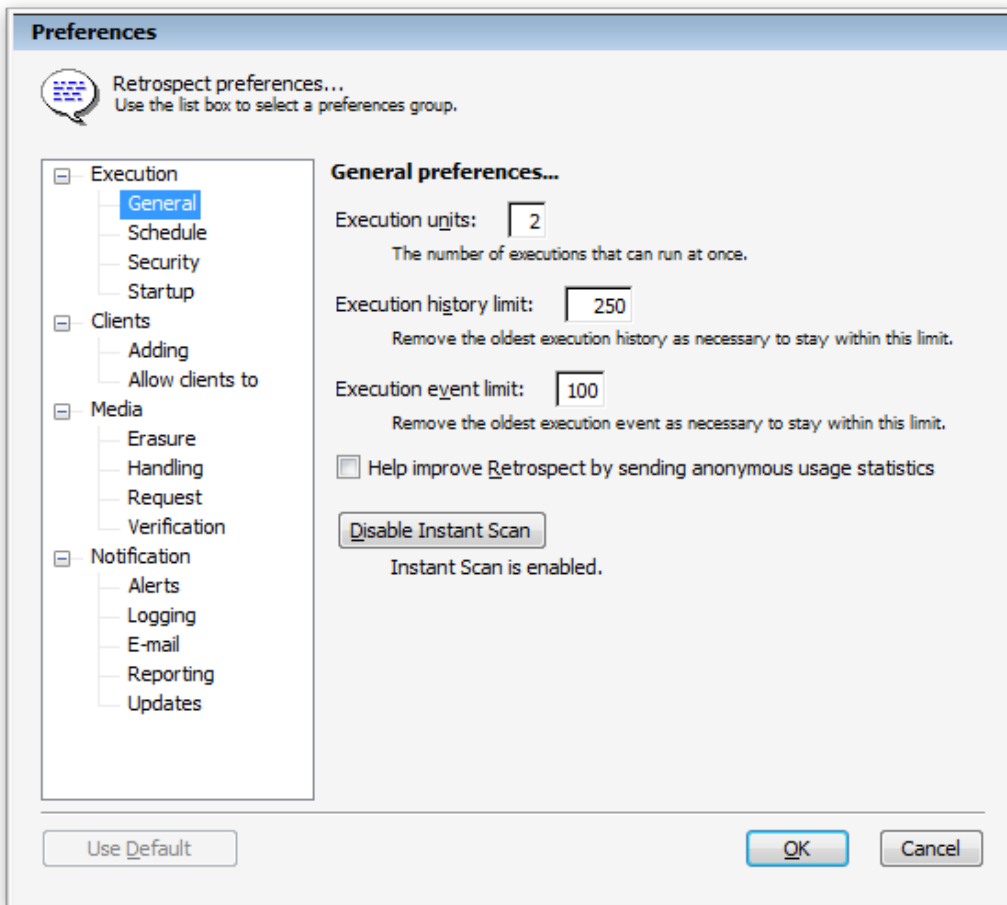




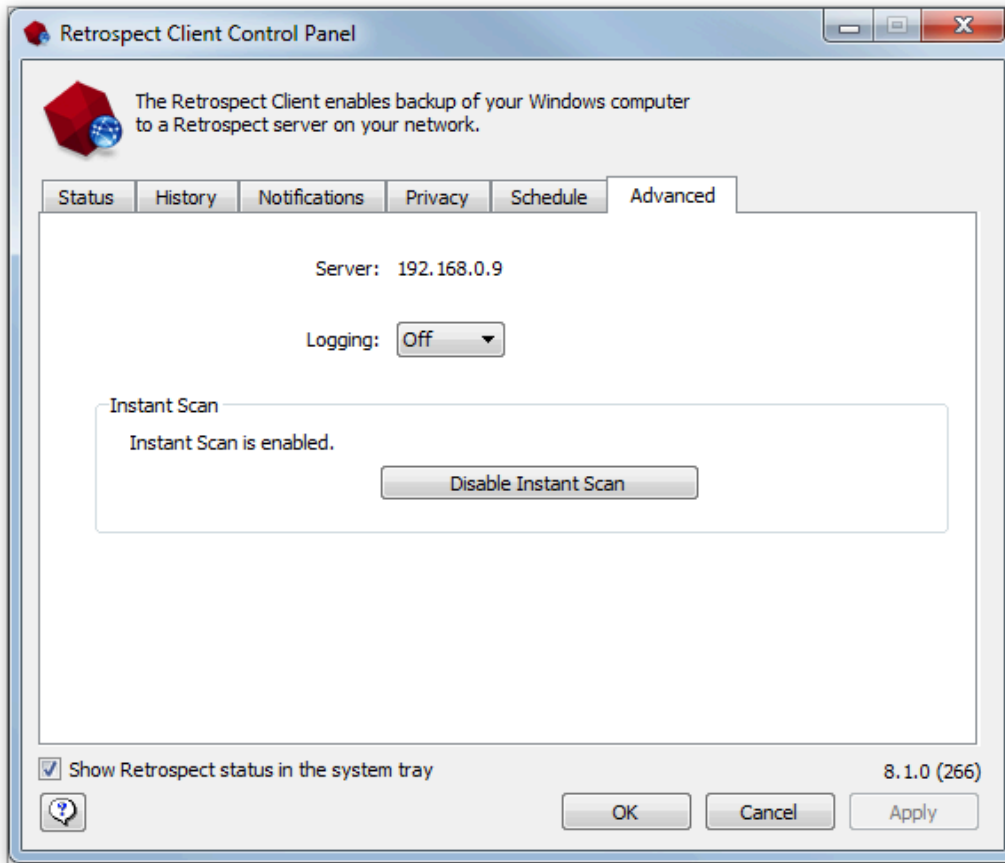
Retrospect Backup 8 for Windows / Retrospect Backup 10 for Mac

You can enable or disable Instant Scan through the user interface for the server and client, whichever is the backup source computer, on both Mac and Windows.

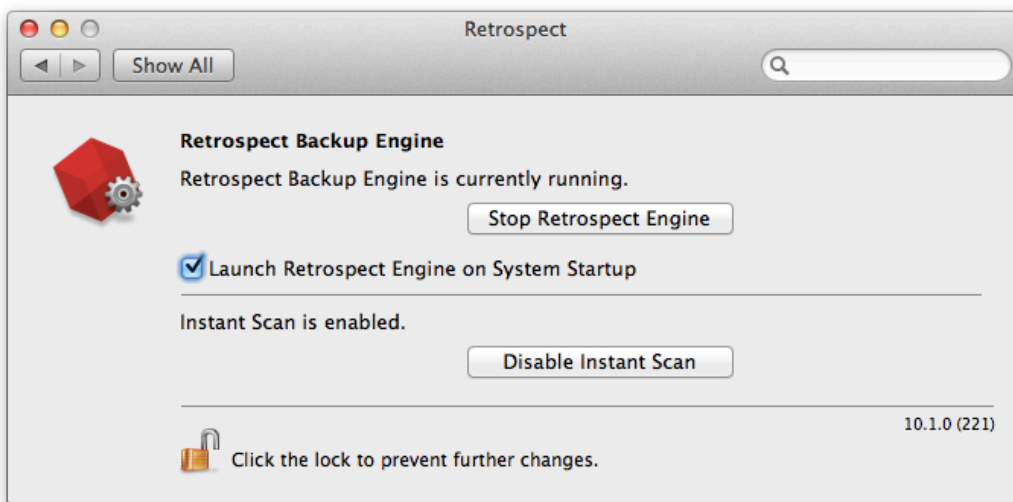
Retrospect for Windows: The option is located in Preferences. Go to *Configure > Preferences > Execution > General* and click "Enable Instant Scan" or "Disable Instant Scan".



Retrospect Client for Windows: The option is located in the Retrospect Client control panel. Open the Retrospect Client. Hold down the ctrl key on the keyboard for two seconds for the Advanced tab to appear. Click Advanced and click "Enable Instant Scan" or "Disable Instant Scan".

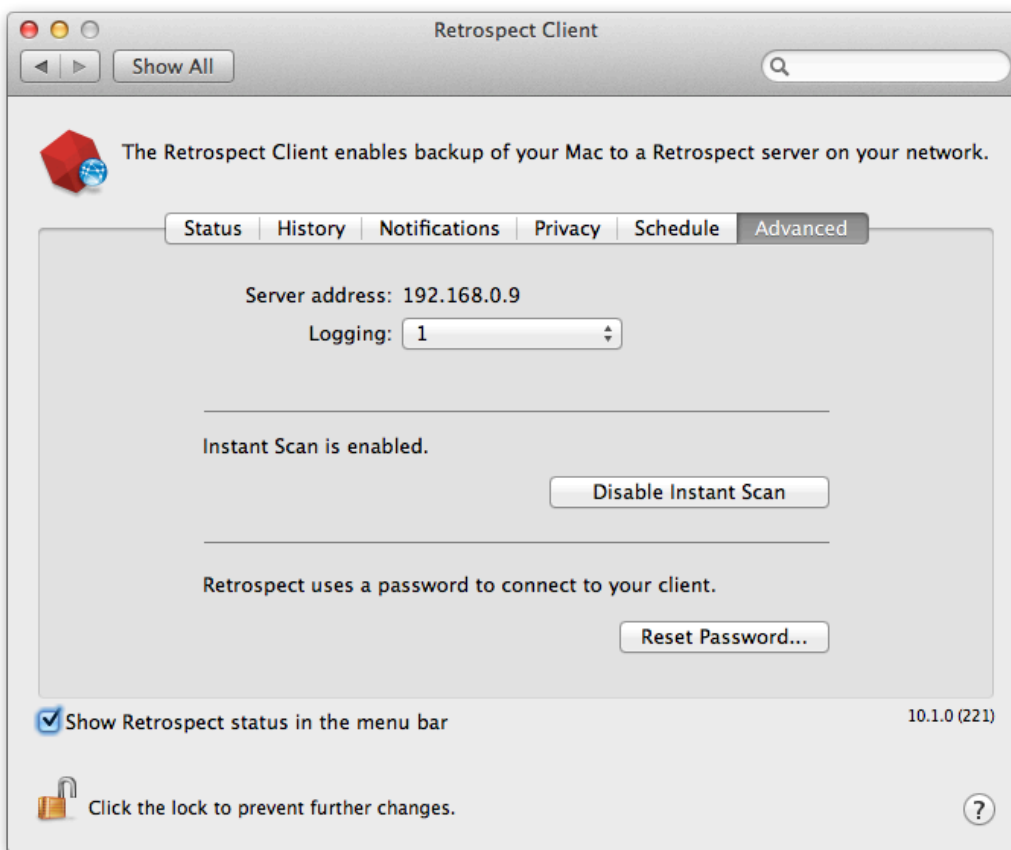


Retrospect for Mac: The option is located in the Retrospect Engine System Preferences pane. Open the Retrospect Engine in system preferences and click "Enable Instant Scan" or "Disable Instant Scan".



Retrospect Client for Mac: Open System Preferences. Hold down the Command key (⌘) on the

keyboard, and click on Retrospect Client. Click the Advanced tab and click "Enable Instant Scan" or "Disable Instant Scan".



launchctl on the Mac

If you have previously used "launchctl unload -w" to disable Instant Scan or "launchctl load -w" to enable Instant Scan on a Mac, this system setting will override the configuration file that Retrospect uses when the computer reboots.

In addition, this setting affects the Retrospect Mac installer for the client and the server. The installer appears to fail with the following message: "The installation failed. The Installer encountered an error that caused the installation to fail. Contact the software manufacturer for assistant." The installer log in the Console utility mentions a "postinstall" issue with the package "com.retrospect.retroisaplist.pkg", resulting in the following error: "install:didFailWithError:Error Domain=PKInstallErrorDomain Code=112". In this case, you should uninstall Retrospect with "Uninstall Retrospect" application included with the console, remove this override setting as described below, and then run the installer again.

To check your system for this setting, open the Terminal application, enter the following, and look for "com.retrospect.retroisa":

```
sudo more /private/var/db/launchd.db/com.apple.launchd/overrides.plist
```

To remove this setting, open the Terminal application and enter the following:

```
sudo /usr/libexec/PlistBuddy -c "Delete :com.retrospect.retroisa" /private/var/db/  
launchd.db/com.apple.launchd/overrides.plist
```

This command will delete an entry in the system's overrides.plist file. You'll be able to enable or disable Instant Scan from the preferences button, and the setting will persist after reboot.

Legacy Client

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.

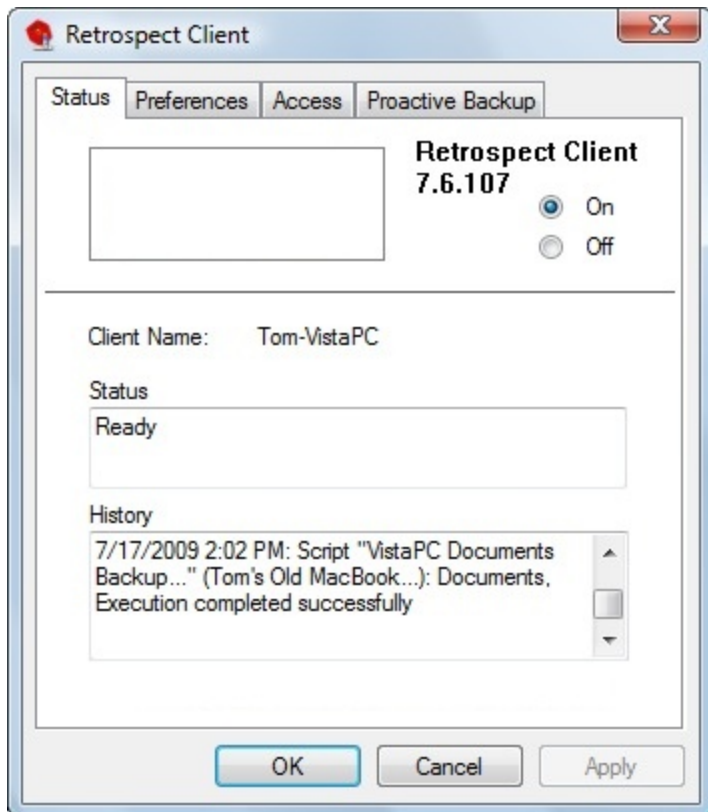
Linux: Run RetroClient.sh from the installed client folder.

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: `$retrocp1 --help`

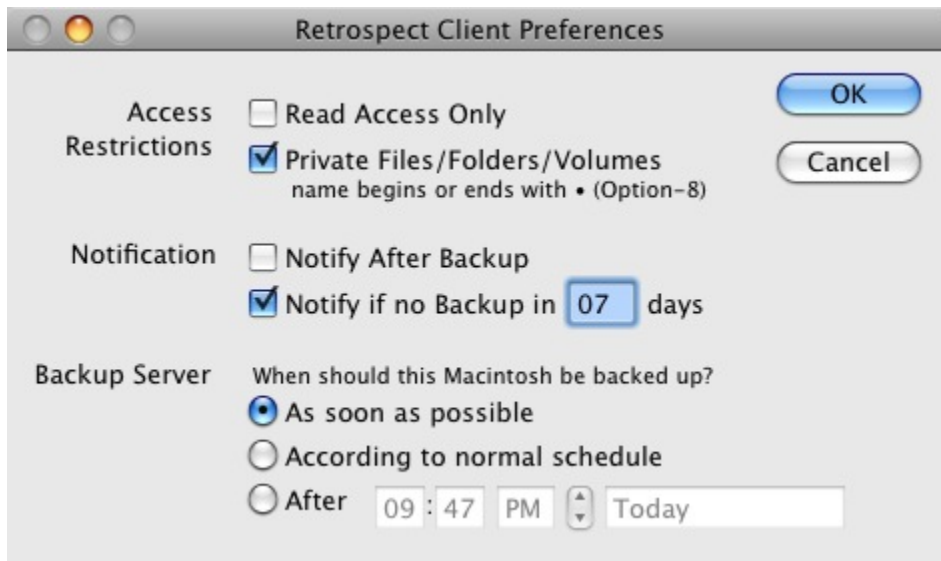
Access Master Control

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.

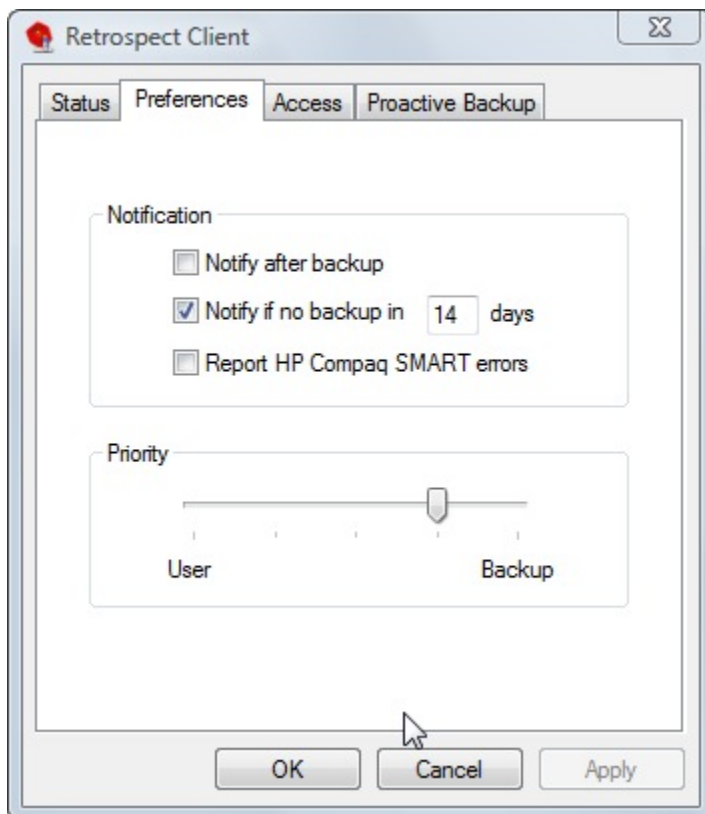
General Preferences

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

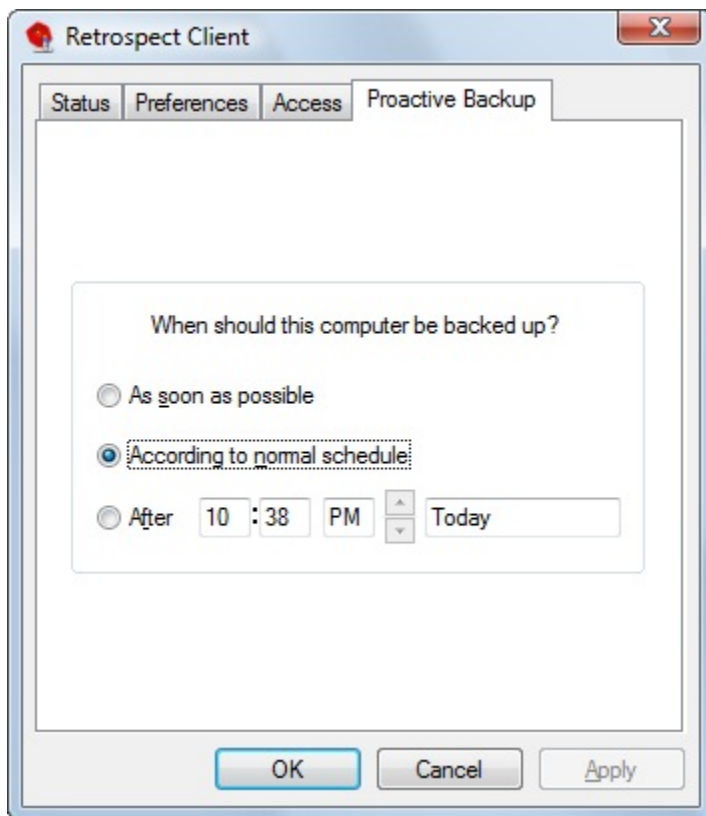
Scheduling from a Client

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.

Client User Preferences

After the client software has been installed, users of client computers can control some aspects of network backup operations with the Retrospect Client control panel.

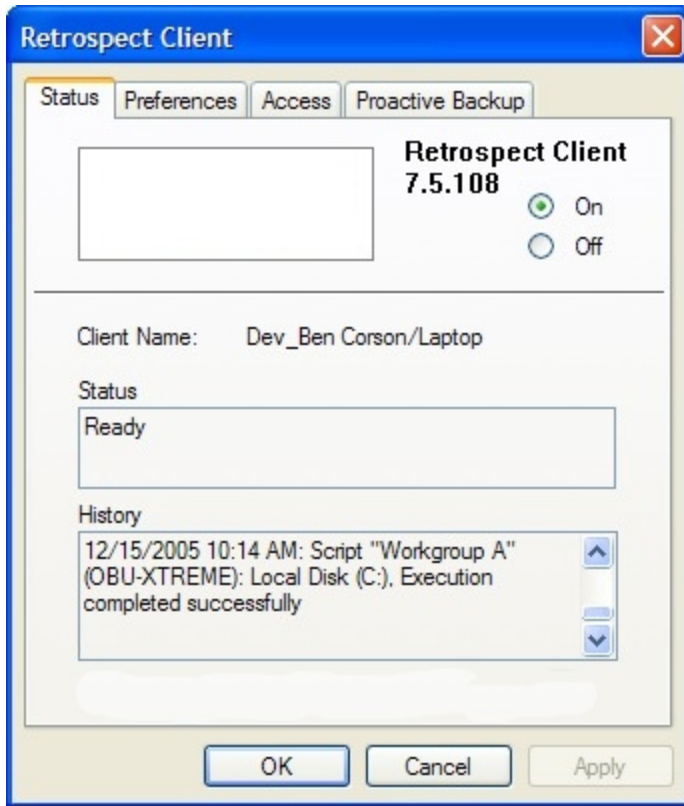
You do not need to change any of the settings to perform backups. In most cases, the existing settings are the ones you will want to use. To open the Retrospect Client control panel, do the following:

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

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

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

The Retrospect Client control panel displays information about the client computer on which it is installed, including the user or computer name, the access status of the client, and a report about the last several backups.



The Windows client control panel, showing the Status tab. (The UNIX client control panel is similar.)



The Mac OS X client application.

In addition to the Java-based graphical user interface, UNIX clients can also be controlled through the command line. To see the command line arguments, enter the following.

```
$retroctl --help
```

Access Master Control

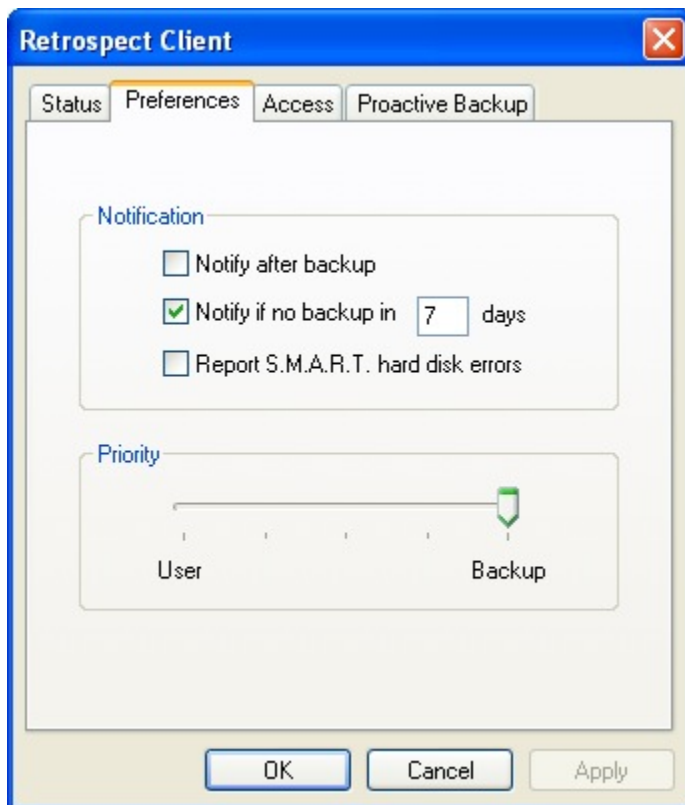
The On and Off radio buttons let you allow or deny network access to your client by the backup computer. When you install the client software and each time the client computer starts up, the control is on to allow access. When the control is turned off, the data on the client computer cannot be accessed over the network by Retrospect.

To permanently prevent access to the client computer, uninstall the Retrospect Client software as described in [Uninstalling a Client and Its Software](#).

General Preferences

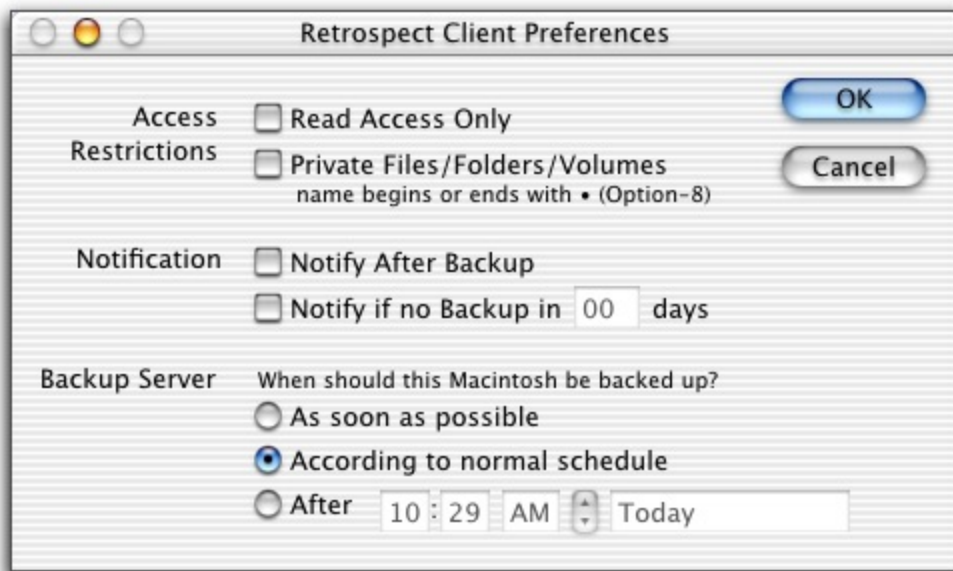
The Retrospect Client control panel has additional user preferences for managing client operations. Getting to the preferences is done differently under Windows/UNIX, and Mac OS.

Windows/UNIX: Click the Preferences tab from the four at the top of the control panel.



The Windows Retrospect Client control panel's preferences.

Mac OS: Click the Preferences button.



The Mac OS X Retrospect Client control panel's preferences.

Wait at Shutdown determines what happens when a client user chooses Shut Down from the Finder's Special menu. When this option is selected and Shut Down is chosen, the "waiting for backup" dialog is displayed until the backup takes place. By default, this preference is selected.

When this dialog is on the client Macintosh screen, the client user may click Restart to restart the client Macintosh, click Shut Down to shut it down, or click nothing and leave it for unattended operation. When the client computer is not used for thirty seconds, a screen saver appears until the user presses a key or moves the mouse to return to the dialog. When the backup computer finishes its operation with this client, it shuts down the client Macintosh.

Run in Background allows the backup computer to operate at the same time the client user is using the client Macintosh. If the check box is not checked, a dialog appears on the client during network operations. This preference is on by default.

When the dialog appears, the user of the client Macintosh can cancel the network operation to continue working or wait until the operation is finished. When "Run in Background" is checked, the dialog does not appear during backups, and the client user can set priority levels for local and network operations. See below for details.

Priority Preference

The priority preference allows the client user to make the client computer favor either the user's task at hand or the operation requested by the backup computer. Under Mac OS, this applies only when the "Run in Background" execution preference is on.

This preference is not available for the Mac OS X client.

Drag the slider and set it to somewhere in the range between "User" and "Backup." When the slider is set all the way to "User," the computer devotes more of its attention to its user, slowing Retrospect client operations slightly. When the slider is set all the way to "Backup," the client operation is given

priority and the client computer is slightly less responsive to its user.

This setting has no effect until the client is actively communicating with the backup computer.

Under Mac OS, the Priority setting is ignored if the client Macintosh is displaying the “waiting for backup” dialog.

Access Restrictions Preferences

These preferences allow the client user to control access to the files and folders on his or her computer.

Read Access Only allows the client computer to be backed up across the network, but prevents writing by the backup computer. This means Retrospect cannot restore, move, or delete files on the client computer, nor can Retrospect be used to rename volumes. The options “Set Volume Backup Date,” “Move Files,” and “Synchronize Clock” cannot be used on the client. This setting is off by default.

Private Files/Folders/Volumes makes any files, folders, or volumes designated as private unavailable to the backup computer. This preference is off by default. Select the check box and designate private items as described below.

To designate an item as private under Windows or UNIX, click the Add button, browse to select the item, then click OK or Exclude. Click Add again to exclude more volumes, folders, or individual files. The privacy feature uses the literal pathnames you specify. If you move or rename a file or folder it may no longer be private. If you mount a volume to a different location, its files and folders may no longer be private.

To designate an item as private under Mac OS, type a bullet (“•”, Option-8) at the beginning or end of its name (placing it at the end will preserve its sort order in the Finder). For example, you could designate the folder “Personal” as private by renaming it “Personal•”.

Notification Preferences

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

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

Notify if no Backup in n days directs the client to display a message after 9:01 *a.m.* if the client has not been backed up within the number of days specified in the entry box. By default, this preference is selected and the number of days is seven.

Report HP Compaq SMART hard drive errors (Windows client only) requests an immediate backup from Proactive Backup (if applicable) when Retrospect learns of errors on the client’s HP Compaq SMART hard drive volumes. By default, this preference is turned on.

Controlling Proactive Backups

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

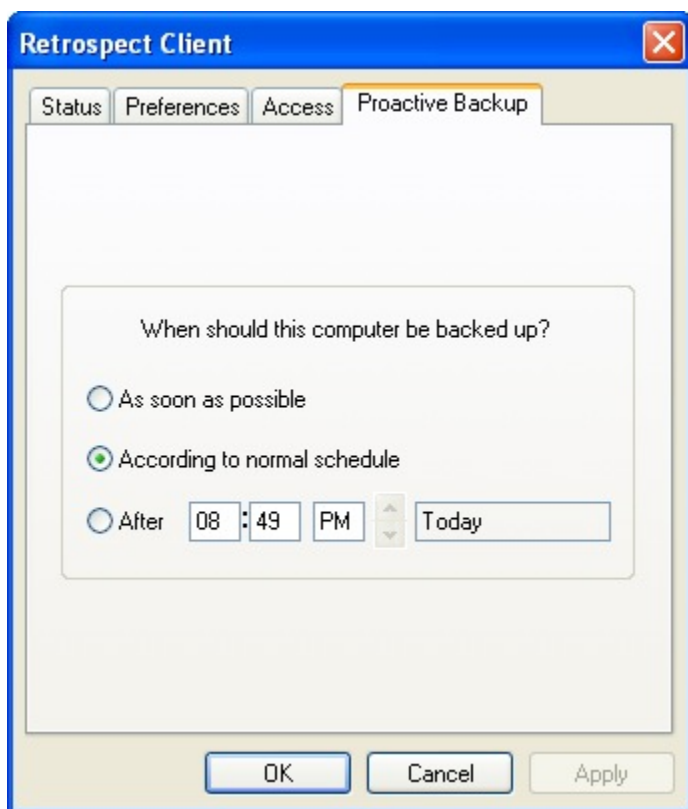
Scheduling from a Client

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.

Proactive Backup is known as the Backup Server on Mac OS client software.

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

Windows/UNIX: Click the Proactive Backup tab to bring its controls to the front.



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

As soon as possible makes the backup computer back up the client computer as soon as the Proactive Backup is available to do so.

According to normal schedule makes the backup computer back up the client computer at its regularly scheduled time in the Proactive Backup script. (This is the default.)

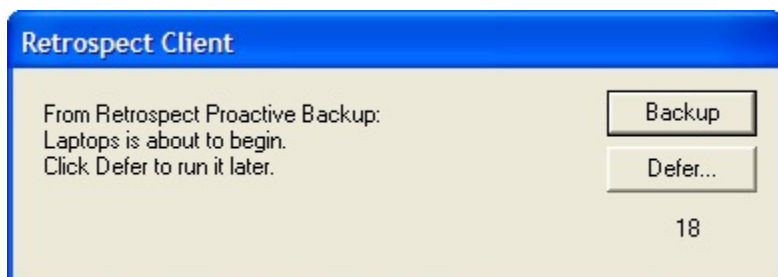
After prevents the backup computer from backing up the client computer before the specified time and date, up to one week from the present time. (Click on the time and date and type or click the

arrows to change them.)

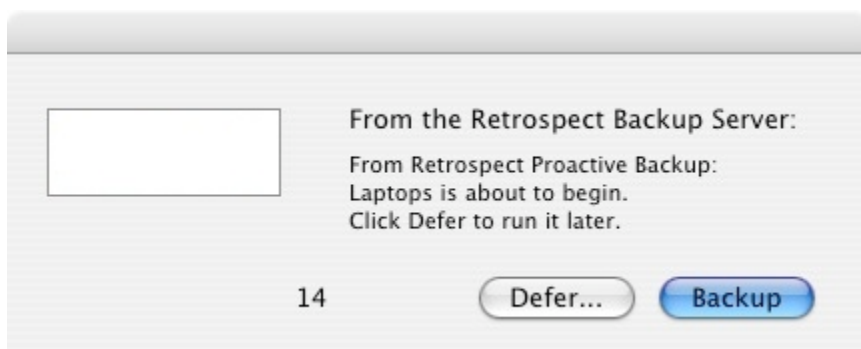
Click OK to accept the settings.

Deferring Execution

When Proactive Backup is about to back up a client, a dialog appears on the screen of the client computer.



Windows/UNIX client Proactive Backup countdown.



Macintosh client Backup Server countdown.

The dialog gives the client user three ways to control the execution of the impending Proactive Backup operation:

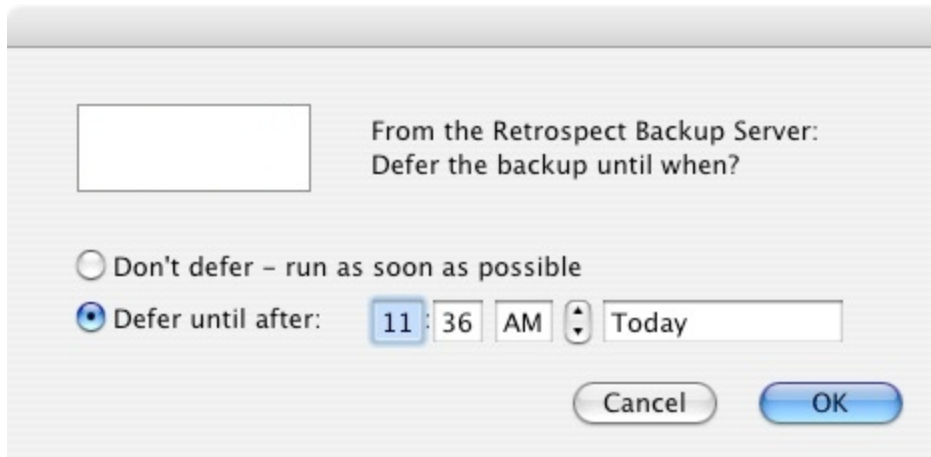
Waiting for the countdown to reach zero allows the Proactive Client Backup to execute.

Clicking **Backup** executes the backup immediately.

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



Deferring the Proactive Client Backup from a Windows or UNIX client.



Deferring the Proactive Client Backup from a Macintosh client.

When a user defers, Retrospect makes an entry in the backup computer's Operations Log.

Glossary

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.

ProactiveAI 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. Previous 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 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 previous 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 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 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.

Release Notes

Every Retrospect release includes numerous bug fixes, as we continue to improve the product's stability, performance, and features. Listed below are a number of resolved issues that our customers have encountered. As always, don't hesitate to contact our support team to report an issue or to check on the status of a known issue. For more information about new features, see [What's New](#).

Windows 19.3.0.132 – March 12, 2024

Versions

Mac console – 19.3.0.132

Mac engine – 19.3.0.132

Mac client – 19.3.0.132

Windows client – 19.3.0.132

Linux client – 19.1.1.102

Script Hooks – 20230816

Engine

IMPROVED Modifying Storage Group properties can take a long time to complete (#10398)

FIXED Error -1001 when backing up OneDrive files in some cases (#7539)

FIXED After a Dropbox connection error, automatic retry doesn't establish a new connection in some cases (#10389)

FIXED Could not extend the immutable retention period of all past backups in cloud Storage Group (#10422)

FIXED Scanning incomplete, error -1020 (sharing violation) when using Open File Backup (#10418)

Mac 19.2.0.122 – October 18, 2023

Versions

Mac console – 19.2.0.122

Mac engine – 19.2.0.122

Mac client – 19.2.0.122

Windows client – 19.2.0.122

Linux client – 19.1.1.102

Engine

- NEW** Support for macOS Sonoma (14.0) - Certified September 26, 2023
- NEW** Media sets no longer created as Storage Groups by default
- FIXED** Object locking retention date is now set during backup set transfer (#10318)
- FIXED** Backups to Dropbox no longer fail when the connection times out (#10387 / Verify/Restore error) - [See details](#)
- FIXED** Storage Group new member data is now always saved to all sub-sets (#10319)
- FIXED** No longer report Unknown Mac error when trying to open offline cloud files (#10349)
- FIXED** Unwanted Public/Private keys no longer created on startup (#10351)
- FIXED** Stop reporting erroneous files no longer present message during backup (#10374)
- FIXED** Fixed assert when internal local volume list maxes out (#9895)
- FIXED** Fixed bad line endings in some Script Hooks example files (#10341)

Console

- NEW** Can now Forget licenses in License preference pane
- IMPROVED** Client update now defaults to correct .rcu file directory(#10345)
- FIXED** Now reporting all licenses are already in use when adding client with a public key (#10348)

Client

- NEW** Mac Client: Support for macOS Sonoma (14.0) - Certified September 26, 2023
- IMPROVED** Windows Client: System tray app now works with high DPI resolutions (#10358)
- FIXED** Mac Client: Fixed issue where clients would go to sleep early in a backup (#6162)
- FIXED** Windows Client: Fixed password issue when adding clients that had been re-installed (#10356)
- FIXED** Windows Client: Fixed issue where public key file was ignored if client already used a password (#10383)

Mac 19.1.1.110 – July 11, 2023

Versions

Mac console – 19.1.1.110

Mac engine – 19.1.1.110

Mac client – 19.1.1.110

Windows client – 19.1.1.110

Linux client – 19.1.1.102

Script Hooks – 20230816

Engine

- IMPROVED** Can now back up OneDrive files in Windows 11 (#10316)
- FIXED** After upgrade, first backup of client source no longer backs up unchanged files (#10300)
- FIXED** Editing Cloud storage group member no longer results in backups going to root of bucket (#10296)
- FIXED** Remembered catalog files now display correct size (#10266)
- FIXED** Backups to Backblaze S3 media sets no longer report misleading HTTP errors (#10304)
- FIXED** Fixed issue with log messages relating to macOS 14 Sonoma (#10329)
- FIXED** Script Hooks: Fixed line endings on macOS shell scripts (#10341)

Client

- IMPROVED** Linux Client: Now supports Rocky Linux and other new distributions - [See details](#)
- FIXED** Linux Client: Client installer can now open firewall on all distributions (#10340)
- FIXED** Mac Client: Fixed issue with log messages relating to macOS 14 Sonoma (#10329)
- FIXED** Windows Client: Can now back up OneDrive files in Windows 11 (#10316)

Mac 19.1.0.219 – December 22, 2022

Versions

Mac console – 19.1.0.219

Mac engine – 19.1.0.219

Mac client – 19.1.0.219

Windows client – 19.1.0.320

Linux client – 19.1.0.102

Engine

- NEW** Support for Retrospect Cloud Storage
- NEW** Backup Comparison for Anomaly Detection
- NEW** OS Compliance Monitoring through Retrospect Management Console
- NEW** Ransomware Protection: Flexible Immutable Retention Periods
- NEW** Cloud Backup: Microsoft Azure for Government
- NEW** Multi-Factor Authentication Option
- NEW** Configuration File Encryption Option
- NEW** Storage Groups: Subset Rebuild
- NEW** Recycle Script Option
- NEW** Support for LTO-9 Tapes
- IMPROVED** Improved Performance for Cloud Backup using Multi-Part Upload
- IMPROVED** 4+ GB File Support for Cloud Replication
- IMPROVED** Back up the same local drive with multiple scripts simultaneously
- IMPROVED** Duplicate/Copy the same local drive with multiple scripts simultaneously
- IMPROVED** Anomaly Detection enabled by default
- IMPROVED** Storage Groups: Group scripts run simultaneously for all subsets
- IMPROVED** Increase maximum execution units from 16 to 64
- IMPROVED** Support: Export log/operation files with configuration files
- FIXED** Sources: Fixed issue where Retrospect did display NTFS drives on macOS Monterey (#10019)
- FIXED** Sources: Fixed icon issue in German (#9419)
- FIXED** Sources: Fixed issue with clock offsets (#10047)

- FIXED** Cloud Backup: Fixed issue with Azure Blob Storage for "Failed to read beginning of SSL/TLS record" (#10267)
- FIXED** Cloud Backup: Fixed issue where new member is incorrectly added during media request (#10138)
- FIXED** Storage Groups: Fixed issue with backed up to members marked as lost (#10233)
- FIXED** Sources: Fixed issue with external ExFAT USB volumes in macOS Ventura (#10236)
- FIXED** Restore: Fixed multiple errors restoring Finder info to DOS volumes on macOS Ventura (#10239)
- FIXED** Cloud Backup: Fixed issue where new member is incorrectly added during media request (#10138)
- FIXED** Storage Groups: Fixed issue with backed up to members marked as lost (#10233)
- FIXED** Cloud Backup: Fixed support for Backblaze's Default Retention Policy (#9821)
- FIXED** Subscriptions: Fixed issue where expiration date not displayed in all cases (#8805)
- FIXED** Rebuild: Fixed performance issue on cloud backup sets (#9214)
- FIXED** Backup: Fixed issue where the last successful backup date not stored after recycle (#9245)
- FIXED** Reporting: add "Immutable Until" for all backup reports (#9281)
- FIXED** ProactiveAI: Fixed issue where policy paused while script being edited (#9860)
- FIXED** ProactiveAI: Fixed issue where policy stops using all available execution units (#10244)
- FIXED** Backup: Fixed remaining issues with DST and "error -2249 (could not find session)" (#10246)
- FIXED** Logging: Better reporting for using cloud storage with default retention date and immutable backups (#9943)
- FIXED** Storage Groups: Fixed issue with restore when selecting catalog for storage group rather than subset (#9961)
- FIXED** Cloud Data Protection: Fixed issue where files in subvolume had unexpected modification date (#9963)
- FIXED** Cloud Data Protection: Fixed UI issues with dates (#10004)
- FIXED** Grooming: Fixed issue with grooming out files based on a selector (#10034)
- FIXED** Cloud Data Protection: Fixed issue duplicating a zero-byte file (#10036)
- FIXED** NAS Backup: Handle incorrect dates from some NAS volumes to enable matching

unchanged files (#10055)

FIXED Cloud Data Protection: Fixed issue with restoring certain files to cloud (#10129)

FIXED Storage Groups: Fixed issue with adding a subset catalog without the main catalog (#10130)

FIXED Scheduling: Fixed issue with day-of-the-week scheduling at 9:00am in certain time zones (#10134)

FIXED SQL Backup: Fixed issue where database clients become unlicensed when busy (#10172)

FIXED Anomaly Detection: Fixed issue where lost members can invoke error (#10234)

FIXED Backup: Fixed issue with backing up data to sets with lost members (#10235)

FIXED Scripts: Fixed issue with "Check Script" when source is a folder (#10245)

FIXED Restore Preflight: Fixed issue with export missing some .rdb file names (#10257)

FIXED Immutable Backups: Fixed issue with transfers from immutable set to local disk set (#10271)

FIXED Transfer Backups: Fixed issue with DST and with recycling source set despite an execution error (#10273)

FIXED Email Notifications: Fixed issue with Microsoft Office 365 for "Failed to read beginning of SSL/TLS record" (#10267)

Client

IMPROVED Mac Client: New "Export Support Logs to Desktop" button in "System Preferences" > "Advanced"

FIXED Mac Client: Fixed issue with log messages relating to macOS Ventura (#10237)

FIXED Mac Client: Fixed issue where client treated Time Machine snapshots as regular volumes (#10277)

FIXED Linux Client: Resolved issue running client alongside Docker (#7547)

ALERT Windows Client: EOL notice for 32-bit client version - [See details](#)

Mac 18.5.3.142 – May 22, 2022

Versions

Mac console – 18.5.3.141

Mac engine – 18.5.3.141

Mac client – 18.5.3.141

Windows client – 18.5.3.142

Linux client – 18.5.3.102

Engine

NEW

Support for macOS Ventura (13.0) - Certified October 24, 2022

FIXED

Alibaba Cloud: Fixed issue where using immutable backups with per-object retention generated an error (#9986)

FIXED

Alibaba Cloud: Added support for creating bucket with retention policy (#9987)

FIXED

ProactiveAI: Fixed issue where ProactiveAI did not alternate between different destinations in Storage Groups (#9995)

FIXED

Azure: Fixed issue where rebuild cloud set on Azure shows Immutable Retention date off by time difference from UTC (#9996)

FIXED

ProactiveAI: Fixed issue where ProactiveAI activities showing wrong destination name for Storage Group in Windows UI (#10005)

FIXED

Tape Rebuild: Fixed "Can't create session, error -2249 (could not find session)" error during catalog rebuild (#10030) - [See details](#)

Client

NEW

Mac Client: Support for macOS Ventura (13.0) - Certified October 24, 2022

FIXED

Linux Client: Fixed ".retroclient -setpass newpass" command (#9983)

FIXED

Linux Client: Fixed issue where new installations did not prompt for password creation (#10022)

ALERT

Windows Client: EOL notice for 32-bit client version - [See details](#)

Mac 18.5.2.120 – March 22, 2022

Versions

Mac console – 18.5.2.120

Mac engine – 18.5.2.120

Mac client – 18.5.2.120

Windows client – 18.5.2.136

Linux client – 18.0.0.103

Engine

IMPROVED Anomaly Detection: Added detailed logging for anomalies

IMPROVED Anomaly Detection: Suppress alerts for rolling synthetic full backups

FIXED Immutable Backups: Clarified immutable retention expiration log message (#9980)

FIXED Daylight Saving Time: Fixed "Trouble matching, error -2249 (could not find session)" error during snapshot transfer (#9981) - [See details](#)

FIXED Client Backup: Fixed engine issue where client errors during building snapshot phase stops the entire script (#9968)

FIXED Management Console: Fixed issue where duplicate scripts had destination mode incorrectly updated (#9964)

FIXED Backup: Fixed issue where Retrospect did not show internal drives when paths matched a share (#9940)

FIXED Script Hooks: Fixed issue where intervention file was not deleted (#9873)

FIXED Transfer Backup Sets: Fixed issue where "Can't access Backup Set, error -703 (need a user-entered password, but can't ask)" error was shown (#9766)

FIXED Sources: Fixed issue where favorite folders on Mac clients did not show up until engine restart (#9681)

FIXED Backup: Fixed issue where engine crashed in rare instances when Linux client connection unexpectedly died (#9969)

Mac 18.5.1.101 – February 15, 2022

Versions

Mac console – 18.5.1.101

Mac engine – 18.5.1.101

Mac client – 18.5.1.101

Windows client – 18.5.1.101

Linux client – 18.0.0.103

Engine

NEW Anomaly Detection - [See details](#)

NEW Support for LTO-9

NEW Immutable Backups: Support for Microsoft Azure Version-Level Locking

NEW Immutable Backups: Bucket Creation Support for Object Lock

FIXED ProactiveAI: Clarified error message where ProactiveAI is paused if script is opened for edit (#9860)

FIXED Backup: Fixed issue where user needs to re-enter encryption password when running Copy Backup script (#9766)

FIXED Remote Backup: Fixed issue where Retrospect did not timeout after remote client disappeared (#9868)

FIXED Grooming: Fixed error -2264 when grooming backups of email account (#9870)

FIXED Restore: Fixed crash using Search for files with backup of the system volume (#9876)

Client

NEW Linux Client: Support for intervention file in Script Hooks - [See details](#)

Mac 18.2.2.242 – December 21, 2021

Versions

Mac console – 18.2.2.242

Mac engine – 18.2.2.242

Mac client – 18.2.2.242

Windows client – 18.2.2.242

Linux client – 18.0.0.103

Engine

FIXED Rebuild: Fixed issue where certain snapshot error during rebuild would stop the rebuild (#6634)

FIXED Clients: Fixed issue where re-installed client needed to be removed and then added again (#9014)

FIXED Backup: Fixed "elem.cpp-1107" crash when backing up macOS sources with "Match only files in same location/path" enabled (#9847)

FIXED Transfer: Fixed "arc.cpp-5798" crash during a transfer that started with a recycle (#9851)

FIXED Transfer: Fixed "-2241 (Catalog File invalid/damaged)" error during certain transfers (#9852)

Console

FIXED Scripts: Fixed issue where under rare conditions, scripts would not show up (#9839)

Mac 18.2.1.241 – November 16, 2021

Versions

Mac console – 18.2.1.241

Mac engine – 18.2.1.241

Mac client – 18.2.1.241

Windows client – 18.2.1.241

Linux client – 18.0.0.103

Engine

NEW Support for Nexsan Unity 7.0 MinIO with Immutable Backups

FIXED Daylight Saving Time: Fixed issue where Retrospect sent too many emails due to time change (#9831)

FIXED Daylight Saving Time: Fixed issue where scripts started one hour early when DST ends (#9830)

- FIXED** Daylight Saving Time: Fixed issue where engine crashed during media verification due to DST (#9832, #9800)
- FIXED** Backup Transfer: Fixed engine crash during snapshot transfer due to bad catalog file (#9807)
- FIXED** Logging: Reduced "Can't copy block level incremental backup file" logging (#9523)
- FIXED** Logging: Reduced "wait time exceeded" logging (#9806)
- FIXED** Logging: Fixed "Can't compress Catalog File for Backup Set" logging (#9833)
- FIXED** Logging: Fixed incorrect logging of media action (#9775)
- FIXED** Storage Groups: Fixed issue where rebuild will fail if .rdb files not in expected location (#9560)
- FIXED** Storage Groups: Fixed rebuild issue where subsets are removed from different storage group (#9808)
- FIXED** Backup Report: Fixed issue where certain ProactiveAI backups were linked to the incorrect destination (#9774)
- FIXED** LTFS: Fixed issue where LTFS tape volumes were not displayed (#9810)
- FIXED** Cloud Storage: Removed incorrect "Trouble deleting files, error -1101 (file/directory not found)" log message (#9778)
- FIXED** Cloud Storage: Fixed rebuild for S3-compatible sets failing for 'Host not found or network unavailable' error (#9715)
- FIXED** Backup: Improved performance of matching for certain use cases (#9818)
- FIXED** Licensing: Fixed crash for rare workflow (#9820)

Client

- FIXED** Mac Client: Fixed "Unsupported version" logging issue in macOS Monterey (#9838)

Mac 18.2.0.168 – September 29, 2021

Versions

Mac console – 18.2.0.168

Mac engine – 18.2.0.168

Mac client – 18.2.0.168

Windows client – 18.2.0.174

Linux client – 18.0.0.103

Engine

NEW

Support for macOS Monterey

NEW

Cloud Backup Certification for IBM ICOS

IMPROVED

Improved Ransomware Protection with Version-Aware Restore

IMPROVED

Improved Dropbox Support with Short-Lived Token Support and Better Security through PKCE - [See details](#)

IMPROVED

Bandwidth Limit Options Support for Cloud Data Protection Support

FIXED

Backup Verification: Fixed issue where media verification disabled immutable retention policy (#9762)

FIXED

Backup Set: Fixed "member index is wrong" error when trying to edit member for a storage group in rare cases (#9606)

FIXED

Rebuild: Fixed catalog rebuild error when a backup is in Daylight Saving Time (DST) but the current time isn't, or vice versa (#9760)

FIXED

Backup Transfer: Fixed error copying a backup that is in DST when the current time isn't, or vice versa (#9656)

FIXED

Backup Transfer: Fixed crash when grooming a cloud set in rare cases (#9573)

FIXED

Ransomware Protection: Fixed log errors when grooming backup set with a retention policy (#9425)

FIXED

Auto-Updates: Fixed issue where automatic upgrades are displayed for more than one version (#9512)

FIXED

ProactiveAI: Fixed issue where disconnected external drives would generate failed activities (#9575)

FIXED

ProactiveAI: Fixed crash when source check threads hang (#9684)

FIXED

ProactiveAI: Fixed rare crash during client scan (#9663)

FIXED

NAS Backup: Fixed issue where cancelling the password prompt for a network share does not stop execution (#9586)

FIXED

Azure: Fixed rare crash when Retrospect fails to connect to Azure (#9736)

FIXED

Cloud Data Protection: Fixed "Trouble deleting files, error -1021 (data overflowed expected amount)" error when duplicating to a Google Cloud bucket (#9758)

Client

NEW

Windows Client: Support for Windows 11

Mac 18.1.1.120 – June 24, 2021

Versions

Mac console – 18.1.1.120

Mac engine – 18.1.1.120

Mac client – 18.1.1.120

Windows client – 18.1.1.106

Linux client – 18.0.0.103

Engine

IMPROVED

Retrospect Management Console Integration with Microsoft Azure Blob Storage

FIXED

ProactiveAI: Fixed issue where failed activities would appear for disconnected data sources with -530 errors (#9486)

FIXED

Grooming: Fixed rare crash for grooming with versioned cloud buckets (#9493)

Client

NEW

Windows Client: Support for Windows Server 2022

Mac 18.1.0.113 – June 17, 2021

Versions

Mac console – 18.1.0.113

Mac engine – 18.1.0.113

Mac client – 18.1.0.113

Windows client – 18.1.0.124

Linux client – 18.0.0.103

Engine

- NEW** Microsoft Azure support
- IMPROVED** Scalable Data Protection - Extended Backup Set Size Limit from 1PB to 1EB
- IMPROVED** Cloud Data Protection: Support for subpaths
- FIXED** Remote Backup: Fixed issue with on-demand backup and restore for certain clients (#9432)
- FIXED** Licensing: Fixed issue where backup to an external hard drive was not possible for certain licenses (#9444)
- FIXED** Licensing: Significantly improved license loading for large number of licenses (#8835)
- FIXED** Tape Backup: Fixed crash when adding members to a set (#9338)
- FIXED** Configuration Management: Fixed issue where rules were not importing correctly (#9473)
- FIXED** Configuration Management: Fixed issue where rules were not importing correctly (#9473)
- FIXED** NAS Support: Fixed issue where duplicating to a NAS with Solo license generated incorrect error (#9433)
- FIXED** Concurrent Executions: Fixed issue where the number of execution units could not be reduced (#9435)
- FIXED** ProactiveAI: Fixed issue where ProactiveAI could not back up from cloud data sources (#9437)
- FIXED** ProactiveAI: Fixed issue when creating a backup set from the wizard (#9438)
- FIXED** ProactiveAI: Fixed rare crash (ex_trigcon.cpp-1696) for concurrent polling with ProactiveAI (#9450)
- FIXED** Cloud Backup: Fixed issue where error showed "Unable to create bucket" instead of "Access denied" (#9451)
- FIXED** Immutable Backup: Fixed issue where catalog rebuild did not preserve the immutable retention policy (#9452)
- FIXED** Backup: Fixed rare crash (tstring.cpp-2385) when backup set is unavailable (#9457)
- FIXED** Restore: Fixed issue where Find Files restore for multiple files results in only 1 file (#9458)
- FIXED** Concurrent Executions: Fixed issue where execution units were reset to 2 for certain licenses (#9459)

Console

IMPROVED Cloud Data Protection: Clarified support for Backblaze B2 in dropdown

IMPROVED Cloud Backup: Clarified support for clouds and added icons in dropdown

Client

NEW Windows Client: Support for Windows 10 May 2021 Update

Mac 18.0.0.397 – May 25, 2021

Versions

Mac console – 18.0.0.397

Mac engine – 18.0.0.397

Mac client – 18.0.0.397

Windows client – 18.0.0.442

Linux client – 18.0.0.103

Engine

NEW Ransomware Protection with Immutable Backups

NEW Security Reporting with Geo Tracking

NEW Improved First Launch Experience

NEW Cloud Data Protection

NEW Cloud-Native Deployment

NEW Cloud Data Protection and Cloud Backup Support for Microsoft Azure – Preview Available – Contact Sales

IMPROVED Dashboard: Add link to Retrospect Management Console

IMPROVED Storage Groups: Enable "Storage Groups" by default

IMPROVED Improve visibility for Full Disk Access

IMPROVED OS: Hide system support macOS volumes

- IMPROVED** Filtering: Excluded more types from compression selector
- IMPROVED** Security: Public/private keypair generation performance dramatically improved
- FIXED** Configuration: Fix engine launch delay and crash after rebuilding from configs.xml (#9217)
- FIXED** Backup: Fixed rare crash during backup due to memory overrun (#9277)
- FIXED** Backup: Fixed issue where engine reports -1115 disk full error instead of displaying a media request (#9239)
- FIXED** Storage Groups: Fixed issue where Use at most value is reset after a catalog rebuild (#9195)
- FIXED** Storage Groups: Fixed "Error -1101 (file/directory not found) can't access catalog file" error from certain workflows (#8381)
- FIXED** Storage Groups: Fixed issue where grooming preference not carried over to new backup sources (#8664)
- FIXED** Storage Groups: Fixed issue with ProactiveAI attempting to write to unavailable destination (#8789)
- FIXED** Storage Groups: Fixed rare issue where backups were stored in wrong location (#9231)
- FIXED** Storage Groups: Fixed rebuild issue with 3+ members (#9292)
- FIXED** Storage Groups: Fixed issue on MinIO for creating storage groups (#9373)
- FIXED** Storage Groups: Fixed issue where spanning set to multiple members (#9294)
- FIXED** ProactiveAI: Fixed issue where backups stuck due to slow source response (#9244)
- FIXED** Rebuild: Fixed issue where process can fail to finish (#9256)
- FIXED** Duplicate: Fixed issue where process can overwrite destination even if newer than source (#9260)

Console

- FIXED** Full Disk Access: Fixed issue where alert was incorrectly displayed when certain custom options were set (#9169)
- FIXED** Scheduling: Fixed issue where backup script schedules did not default to Monday (#9309)

Client

- NEW** Windows Client: Support for Windows 10 October 2020 Update

NEW

Windows Client: Support for Windows Server 2022 Preview

FIXED

Linux Client: Fixed issue where create date metadata is getting set to default start date for files copied from Linux client (#9317)

Mac 17.5.2.103 – December 9, 2020

Versions

Mac console – 17.5.2.103

Mac engine – 17.5.2.103

Mac client – 17.5.0.185

Windows client – 17.5.0.237

Linux client – 17.0.1.132

Engine

FIXED

Cloud Backup: Fixed rare crash for cloud uploads (#9082)

Console

FIXED

Fixed issue where Full Disk Access alert was incorrectly displayed when certain custom options were set (#9169)

Client

FIXED

Windows Clients: Fixed issue where certain restores to Windows 7 resulted in "File appears incomplete" errors (#9134)

FIXED

Linux Clients: Fixed issue where the client ignored certain mount points (#8985)

Mac 17.5.1.101 – October 7, 2020

Versions

Mac console – 17.5.1.101

Mac engine – 17.5.1.101

Mac client – 17.5.0.185

Windows client – 17.5.0.237

Linux client – 17.0.1.132

Engine

FIXED

Backup: Fixed issue that prevented simultaneous operations to storage groups (#8893)

Mac 17.5.0.185 – September 23, 2020

Versions

Mac console – 17.5.0.185

Mac engine – 17.5.0.185

Mac client – 17.5.0.185

Windows client – 17.5.0.237

Linux client – 17.0.1.132

Engine

NEW

Cloud Certifications: Amazon S3 Virtual-Host Style paths - [See details](#)

NEW

Cloud Certifications: Alibaba Cloud

NEW

Cloud Certifications: Backblaze B2's S3 API

NEW

Cloud Certifications: Webair

NEW

Apple macOS Big Sur Support

NEW

Apple Silicon/M1 Support (using Rosetta)

FIXED

Transfer Backup: Fixed issue where transfer snapshot with multiple sources did not properly close set after use (#8737)

FIXED

ProactiveAI: Fixed issue where backups could run even when script is inactive (#8739)

FIXED

Storage Groups: Fixed issue where backing up to a storage group while transferring results in -843 error (#8821)

Console

FIXED

Performance: Fixed issue where console could hang under certain ProactiveAI workloads (#8660)

FIXED

Memory Footprint: Reduced memory usage for console during operations (#8806)

Client

FIXED

Restore-on-Demand: Fixed issue where restoring to a different folder changes its permissions (#8603)

Mac 17.0.2.101 – May 13, 2020

Versions

Mac console – 17.0.2.101

Mac engine – 17.0.2.101

Mac client – 17.0.2.101

Windows client – 17.0.2.102

Linux client – 17.0.1.132

Engine

FIXED

Storage Groups: Fixed issue where grooming a storage group can fail (#8674)

FIXED

Storage Groups: Fixed issue where rebuilding a storage group can fail to delete previous catalog (#8672)

Client

NEW

Windows Client: Windows 10 May 2020 Update certification (Added June 2)

Mac 17.0.1.141 – May 1, 2020

Versions

Mac console – 17.0.1.141

Mac engine – 17.0.1.141

Mac client – 17.0.1.141

Windows client – 17.0.1.165

Linux client – 17.0.1.132

Engine

- IMPROVED** Disaster Recovery support for Mojave and Catalina - [See details](#)
- IMPROVED** Disaster Recovery redesigned workflow for El Capitan, Sierra, and High Sierra - [See details](#)
- IMPROVED** Restore Preflight: Include "First RBD" and "Last RDB" (#8486)
- FIXED** Storage Groups: Fixed issue where Copy Media Set to storage group failed to report error that catalog file not be found (#8414)
- FIXED** Storage Groups: Fixed issue where skip to new member failed if source hadn't been backed up before (#8506)
- FIXED** Storage Groups: Fixed issue where grooming did not list correct set name in logging (#8575)
- FIXED** Storage Groups: Fixed issue with rebuild for storage group not at the root of a drive (#8581)
- FIXED** Storage Groups: Fixed "error -1 (unknown)" error for grooming certain storage groups (#8623)
- FIXED** Storage Groups: Fixed issue with media requests on certain backups (#8574)
- FIXED** Storage Groups: Fixed issue with "Use At Most" being incorrect for certain backups (#8593)
- FIXED** Storage Groups: Fixed unicode support in storage group names (#8585)
- FIXED** Storage Groups: Fixed issue where "LmGet: ndex = 0 < 1" appears in logs when exporting Backup Report (#8648)
- FIXED** Storage Groups: For grooming, show correct activity name and type (#8650)
- FIXED** Backup: Fixed issue where the incorrect path is used for backup sets and storage groups in rare cases (#8480)
- FIXED** Backup: Fixed issue where large destinations sporadically caused incorrect media requests (#8632)
- FIXED** ProactiveAI: Fixed issue where multiple scripts with the same source would hang the discovery process (#8624)
- FIXED** ProactiveAI: Fixed issue where dialog appeared for clients not found on network (#8547)
- FIXED** ProactiveAI: Fixed memory leak during polling (#8635)
- FIXED** Subscriptions: Fixed issue where expiration date was not updated correctly for certain engines (#8475) - [See details](#)

- FIXED** Remote Backup: Fixed issue where link encryption prevented backup (#8395)
- FIXED** Remote Backup: Fixed issue with not logging out clients after ProactiveAI backup (#7967)
- FIXED** Configuration: Fixed issue where Retrospect hung backups during export (#8454)
- FIXED** Configuration: Fixed issue where corrupted configuration file would cause engine to not start (#8556)
- FIXED** License Manager: Fixed issue where new application license is rejected (#8474)
- FIXED** License Manager: Fixed issue where user could enter multiple licenses (#4663)
- FIXED** Backup-on-Demand: Cloud sets now supported (#8511)
- FIXED** Client Update: Fixed issue where updating client manually caused client to need re-installation (#8530)
- FIXED** NAS Shares: Fixed hang while browsing share with incorrect permissions (#8597)
- FIXED** NAS Shares: Fixed issue for exported configuration of NAS share paths (#8600)
- FIXED** Install Retrospect: Updated icon to red for Dark Mode support (#8559)
- FIXED** Install Retrospect: On upgrade, rename and preserve existing configuration file (#8566)
- FIXED** Rebuild: Fixed issue where operation scanned folders outside of the set (#8555)

Console

- IMPROVED** Dashboard: Full support for Dark Mode
- IMPROVED** Better alerts for Full Disk Access - [See details](#)
- FIXED** Dashboard: Fixed issue with blank view for unsupported languages (#8376)
- FIXED** Dashboard: Fixed issue with source names containing double quotes (#8652)

Client

- NEW** Linux Client: Added AES-256 link encryption to match Windows client and Mac client
- FIXED** Mac Client: Fixed issue where binding the IP meant client would show up as not connected (#8133)

Mac 17.0.0.149 – March 3, 2020

Versions

Mac console – 17.0.0.149

Mac engine – 17.0.0.149

Mac client – 17.0.0.149

Windows client – 17.0.0.180

Linux client – 17.0.0.101

Management Console

- NEW** Dashboard displays status for backup engines
- NEW** Automatic Onboarding for Servers and Endpoints
- NEW** Automatic Onboarding for Retrospect Backup engines
- NEW** Automatic Onboarding for Retrospect Virtual

Engine

- NEW** Automatic Onboarding with Retrospect Management Console
- NEW** Nexsan E-Series/Unity Certification
- NEW** 10x Faster ProactiveAI
- NEW** Restore Preflight
- IMPROVED** Installation: Installer has been simplified to "Install Retrospect" to install Console and Engine
- IMPROVED** Client Discovery: Support for per-minute polling
- FIXED** Storage Groups: Fixed UI issue for backing up more than one source and -843 log issues (#7951)
- FIXED** Storage Groups: Fixed issue with skipping to a new member for cloud members (#8204)
- FIXED** Storage Groups: Fixed issue with backing up to a storage group that is being rebuilt (#7959)
- FIXED** Storage Groups: Fixed issue with large rebuilds of storage groups reporting a missing sub-catalog (#8063)
- FIXED** Storage Groups: Fixed -843 error during snapshot transfer (#8124)
- FIXED** Storage Groups: Fixed issue with multiple write access to the same catalog file (#8373)

- FIXED** Automatic Updates: Fixed issue where client update process incorrectly reports as failed with error -562 (network connection reset by peer) (#7957)
- FIXED** Configuration Management: Fixed issue with importing certain subvolumes from configs.xml (#7848)
- FIXED** Logging: Fixed timezone/daylight saving time issue (#8228)
- FIXED** Cloud Backup: Fixed issue where backup will ask for media after member size has been increased (#8282)
- FIXED** Cloud Backup: Fixed issue where certain local cloud rebuilds failed (#8423)
- FIXED** Cloud Backup: Fixed issue where Dropbox performance was slower than expected (#8458)
- FIXED** Cloud Backup: Fixed issue with AWS S3 API signature v2 support (#8520)
- FIXED** Email Backup: Fixed issue where files chosen showed incorrect value for what is being overwritten (#8298)
- FIXED** Backup: Fixed crash for names that contain specifier characters such as %T (#8379)
- FIXED** Backup: Fixed issue with daylight saving time and timezones (#8289)
- FIXED** Transfer: Fixed issue where transfer backup set transferred more snapshots than required (#8404)
- FIXED** Grooming: Fixed issue where groom failure could cause catalog errors after a rebuild (#8457)

Console

- NEW** Onboarding: Option to send public key to Management Console automatically
- FIXED** Sources: Add > Test Address button now returns client information (#8468)
- FIXED** Backup Sets: Updated "Capacity" and "Free" calculations for disk and cloud media sets (#8090)

Mac 16.6.0.114 – December 2, 2019

Versions

Mac console – 16.6.0.114

Mac engine – 16.6.0.114

Mac client – 16.5.1.104

Windows client – 16.5.1.109

Linux client – 16.0.0.107

Console

NEW

Retrospect Console Preview - [See details](#)

FIXED

Fixed Dark Mode for Restore Assistant "Find Files" (#8380)

Engine

FIXED

Management Console Integration: Fixed issue where customers with many old backup sets are not able to use site (#8336)

FIXED

Email Protection: Fixed issues with large-scale restores from Gmail to Office 365 (#8280)

FIXED

Catalina Support: Fixed issue where "home" incorrectly showed up as a source (#8258)

FIXED

Storage Groups: Fixed issue with copy scripts not transferring the most recent backups (#8296)

Client

FIXED

Mac Client: Fixed crash for client volumes with names longer than 27 characters (#8322)

FIXED

Mac Client: Fixed issue where engine did not log error for unsupported 10.6 clients (#8346)

FIXED

Linux Client: Fixed crash for clients using GLIBC less than 2.14 (#8317)

Mac 16.5.1.104 – October 16, 2019

Versions

Mac console – 16.5.1.104

Mac engine – 16.5.1.104

Mac client – 16.5.1.104

Windows client – 16.5.1.109

Linux client – 16.0.0.107

Management Console

- FIXED** Sources: Added icon for Exchange databases (#8261)
- FIXED** Sources: Added icon for emailaccounts (#8266)
- FIXED** Sources: Fixed issue with how Linux volume is displayed (#8262)
- FIXED** Scripts: Correctly identify destinations are storage groups (#8267)
- FIXED** Dashboard: Fixed incorrect grouping for backup sets under "Storage Predictions" in an organization (#8259)
- FIXED** Dashboard: Names with ellipses display entire name with hover (#8260)

Engine

- FIXED** Sources: Fixed issue where Retrospect shows the same mounted share twice (#8276)
- FIXED** Scripts: Fixed issue where schedules are not imported correctly using configuration file (#8300, #8303)

Console

- FIXED** macOS Catalina: Fixed icons under non-retina screens (#8292)

Client

- NEW** Windows Client: Windows 10 November 2019 Update certification

Mac 16.5.0.169 – October 1, 2019

Versions

Mac console – 16.5.0.169

Mac engine – 16.5.0.169

Mac client – 16.5.0.169

Windows client – 16.5.0.218

Linux client – 16.0.0.107

Management Console

- NEW** Redesigned interface for larger environments - [See details](#)
- NEW** New Scripts View
- NEW** New Sources View
- NEW** New Backup Sets View
- NEW** New Activities View
- NEW** Ability to create and edit scripts on a specific engine
- NEW** Ability to create and edit backup sets for disk, NAS, and cloud on a specific engine

Engine

- NEW** Apple macOS Catalina support (pending final release) - [See details](#)
- NEW** Cloud certification for Backblaze B2 EU Data Center
- IMPROVED** Improved NAS support with auto-adding existing NAS share mounts
- IMPROVED** Retrospect Solo supports NAS volumes
- IMPROVED** Client scanning 2× faster
- IMPROVED** Support for 4 million folders on a single volume
- FIXED** Storage Groups: Fixed issue where backup went to incorrect sub-catalog in rare instances (#7791)
- FIXED** Storage Groups: Fixed issue where media verification did not work properly in certain situations (#8100)
- FIXED** Storage Groups: Fixed issue with matching in Copy Media Set and Copy Backup scripts (#8131)
- FIXED** Storage Groups: Fixed issue where master catalog was not correct after rebuild of multiple members (#8146)
- FIXED** Storage Groups: Fixed issue for rebuilding cloud sets with multiple members (#8168)
- FIXED** Storage Groups: Fixed issue where UI did not display correct information after a cloud storage group rebuild (#8215)
- FIXED** Script: Fixed issue where customer could not add backup to Copy Backup script (#8105)

FIXED Cloud Backup: Enable retry mechanism when getting network error during upload to Backblaze B2 (#8130)

FIXED Email Backup: Fixed issue for restoring more email than expected after a previous restore (#8176)

FIXED NAS Support: Fixed issue where "Copy only missing files" still copied files with certain attributes (#5354)

FIXED NAS Support: Fixed error "MapError: unknown Mac error 34" during scanning of certain files (#8242)

FIXED NAS Support: Fixed issue where Restore/Copy created empty symlink under SMB (#8232)

Console

FIXED Dark Mode: Fixed predicate editor and scope button views (#8195)

FIXED Activities: Fixed issue where user could not choose existing set for media request (#8233)

Client

FIXED Linux: Resolved error "fetFileSpec: ExtAttrGetData (error 61)" during client backup, no client update required (#8112)

FIXED Mac: Fixed issue where scan of files or folders with long non-English names resulted in incomplete scan (#8134)

FIXED Mac: Fixed issue where client's saved IP address not displayed properly in log as "saved ip address is" (#8132)

Mac 16.1.2.102 – May 28, 2019

Versions

Mac console – 16.1.2.102

Mac engine – 16.1.2.102

Mac client – 16.1.0.134

Windows client – 16.1.0.158

Linux client – 16.0.0.107

Engine

FIXED Storage Groups: Fixed issue with configuration import for Storage Groups (#8126)

FIXED NAS: Fixed issue where certain NAS devices could no longer be found (#8121)

FIXED Storage Groups: Fixed logging issue where Storage Groups added many entries for "reserve failed; error -843 (resource is in use by another operation)" (#8122)

Mac 16.1.1.100 – May 20, 2019

Versions

Mac console – 16.1.1.100

Mac engine – 16.1.0.134

Mac client – 16.1.0.134

Windows client – 16.1.0.158

Linux client – 16.0.0.107

Engine

FIXED Storage Groups: Fixed rare issue where certain backups are incomplete (#8102)

Mac 16.1.0.134 – May 14, 2019

Versions

Mac console – 16.1.0.134

Mac engine – 16.1.0.134

Mac client – 16.1.0.134

Windows client – 16.1.0.158

Linux client – 16.0.0.107

Engine

NEW Retrospect Management Console: Pause/Unpause/Stop support

NEW Retrospect Management Console: Versions, Editions, Platforms listed

IMPROVED Retrospect Management Console: Disable deployment for an existing shared script

IMPROVED Email Notifications: stopped scripts now generate email with title "Execution stopped by operator - Retrospect"

FIXED Storage Groups: Fixed issue where the engine would not consistently find all catalogs during a rebuild (#8075)

FIXED Storage Groups: Fixed issue where "Copy Backup" did not work with storage groups (#8094)

FIXED Storage Groups: Fixed issue where rebuild failed silently with improperly named catalogs with "number dash" (#8080)

FIXED Storage Groups: Fixed issue with importing XML configuration with Storage Group (#7973)

FIXED Backup Set Transfer: Fixed issue where transfer across media with errors resulted in incorrect restores (#8085)

FIXED Tape: Fixed issue where the capacity was incorrect after set creation (#8067)

Console

FIXED Sources: Added a smart tag for "All Email" (#7421)

Client

NEW Windows Client: Windows 10 May 2019 Update certification

Mac 16.0.2.101 – April 11, 2019

Versions

Mac console – 16.0.2.101

Mac engine – 16.0.2.101

Mac client – 16.0.2.101

Windows client – 16.0.2.101

Linux client – 16.0.0.107

Engine

FIXED Management Console: Fixed issue where "Deployed On" was not getting the correct date

from the engine (#8012)

FIXED Storage Groups: Grooming is not automatically running when a set runs out of space (#8052)

FIXED Rebuild: Fixed issue where disk set rebuild would leak file handles and eventually run out (#8029)

FIXED Rebuild: Now permitted to run when program is deferred (#8032)

FIXED ProactiveAI: Fixed issue where sources are left in an incorrect state during ProactiveAI backup (#8064)

FIXED Signing: Fixed issue where in rare cases an empty retro.ini file is created inside engine bundle, breaking the signature (#8044)

Console

FIXED Preferences: "Export Client" and "Export Server installer and uninstaller" are now available under Console (#8036)

Mac 16.0.1.105 – March 28, 2019

Versions

Mac console – 16.0.1.105

Mac engine – 16.0.1.105

Mac client – 16.0.1.105

Windows client – 16.0.1.103

Linux client – 16.0.0.107

Engine

FIXED Storage Groups: Backup of offline client results in correct error message (#7923)

FIXED Storage Groups: Manual recycle now logs master catalog name (#7938)

FIXED Storage Groups: ProactiveAI now correctly uses Wake-On-LAN (WOL) packets (#8005)

FIXED Storage Groups: Fixed issue for rebuilding a disk set with multiple members in the same directory (#8019)

FIXED Storage Groups: Fixed issue where rebuild did not preserve grooming settings (#7994)

- FIXED** Storage Groups: Fixed rare crash for arc.cpp-2490 during thorough catalog rebuild (#7978)
- FIXED** Storage Groups: Fixed issue where sub-catalogs were being orphaned on startup (#7990)
- FIXED** Client Autoupdate: process waits for all operations on a client to complete before starting (#7953)
- FIXED** Backup Sets: Fixed issue where backup wizard gave error 0 when trying to save to a share (#7996)
- FIXED** Backup Sets: Fixed issue where rebuild did not work for certain sets (#8011)
- FIXED** Logging: Added missing localizations for certain log messages (#8009)
- FIXED** Past Backups: Fixed issue with retrieving multiple backups with Windows state data in them (#7931)
- FIXED** Backup: Fixed crash on macOS 10.9 or older with certain settings in INI (#8003)

Console

- FIXED** Storage Groups: Fixed issue where checkbox hidden in localized versions (#8007)
- FIXED** Storage Groups: Fixed "Lost" checkbox in Members (#7980)

Client

- IMPROVED** Windows: retroclient.exe -params outputs to stdout

Mac 16.0.0.189 – March 5, 2019

Versions

- Mac console** – 16.0.0.189
- Mac engine** – 16.0.0.189
- Mac client** – 16.0.0.189
- Windows client** – 16.0.0.224
- Linux client** – 16.0.0.107

Engine

- NEW** Retrospect Management Console - [See details](#)
- NEW** Storage Groups - [See details](#)
- NEW** Deployment Tools - [See details](#)
- NEW** Support for Exchange 2019
- NEW** Support for SQL Server 2019 (CTP 2)
- NEW** Cloud Protection: certification for MCT
- NEW** Cloud Protection: certification for IONOS
- NEW** Cloud Protection: certification for Orange Cloud for Business
- IMPROVED** Scanning faster on APFS volumes
- FIXED** Email Reporting: Fixed issue with very large environments (#7698)
- FIXED** Email Reporting: Fixed issue where email accounts were not included (#7723)
- FIXED** Email Protection: Fixed rare crash during backup (#7822)
- FIXED** Email Protection: Tree view no longer display incorrect dates if "Date" field not found in message (#7759)
- FIXED** Cloud Backup: Fixed issue with "-802: Sorry, can't save configuration during backup" (#7845)
- FIXED** Cloud Backup: Fixed issue with "Error -692 (mismatched persistent data) log entries" (#7860)
- FIXED** Logging: Fixed issue where operations log was not searchable (#7324)

Client

- IMPROVED** Mac: Client scanning faster on APFS volumes
- FIXED** Mac: Client uninstaller now removes /var/tmp/retro_ip (#7758)
- ALERT** Mac: EOL notice for Apple Mac OS X 10.3, 10.4, and 10.5 - [See details](#)

Mac 15.6.1.105 – November 29, 2018

Versions

Mac console – 15.6.1.105

Mac engine – 15.6.1.105

Mac client – 15.6.1.105

Windows client – 15.6.1.104

Linux client – 15.1.2.101

Engine

FIXED Remote Backup: Fixed issue where remote backup failed if client added by name (#7705)

FIXED Remote Backup: Fixed issue where remote backup connection was incorrectly closed (#7735)

FIXED Remote Backup: Fixed issue where Retrospect would not time out when searching for a remote backup client (#7748)

FIXED Remote Backup: Fixed rare crash for certain scenarios (#7740)

FIXED Email Protection: Fixed restore issue for certain .eml files on Mac

FIXED Backup: Fixed scanning issue where /home is symlinked to a NAS share (#7744)

FIXED Backup: Fixed assert for rare scenario (#7741)

FIXED Backup: Fixed issue where scripts hung due to Management Console integration (#7753)

Client

NEW Windows Client: New Client API for on/off state

NEW Linux Client: System Certification for CentOS 7.5

IMPROVED Windows: Command-line interface now supports "retroclient.exe -parms" command

Mac 15.6.0.125 – October 16, 2018

Versions

Mac console – 15.6.0.125

Mac engine – 15.6.0.125

Mac client – 15.6.0.125

Windows client – 15.6.0.135

Linux client – 15.1.2.101

Engine

NEW

Management Console Beta Integration - [See details](#)

NEW

Email Protection for IceWarp - [See details](#)

IMPROVED

Improved Support for macOS Mojave

FIXED

Mojave: Installer updated to support Mojave features when installed under 10.8+ to handle OS upgrade after Retrospect upgrade (#7677)

FIXED

Mojave: Fixed icons for RetrospectEngine.app and RetrospectInstantScan.app (#7603)

FIXED

In-App ASM: Expiration date should be fetched from licensing server immediately when entered (#7604)

FIXED

In-App ASM: Fixed descriptions for certain ASM license codes (#7687)

FIXED

In-App ASM: Fixed issue with trials expiring based on ASM expiration date of previous license (#7663)

FIXED

In-App ASM: Fixed issue where customer would get expiration alert when entering valid ASM license (#7665)

FIXED

Subscriptions: Switching to permanent license now removes subscription status (#7609)

FIXED

Storage Groups: Support for email backup (#7618)

FIXED

Storage Groups: Fixed issue with using paths above 60 characters for destinations (#7658)

FIXED

Storage Groups: Support for Add/Locate after it has been forgotten (#7645)

FIXED

Storage Groups: Support for adding and removing members (#7602)

FIXED

Licensing: Fixed issue where user could add multiple application licenses (#7652)

FIXED

Scanning: Update progress promptly during slow scan of certain NAS volumes with many files (#7653)

FIXED

Building Snapshot: Fixed hang when client disconnects in the middle (#7656)

FIXED

Scripts: Fixed issue with running script with "%" in name causing a crash in media request (#7674)

FIXED Email Protection: Fixed issue where Retrospect compared messages in wrong folders when copying entire volume (#7453)

FIXED Email Protection: Fixed restore issue to a subvolume on a Dovecot server causing error "Mailbox doesn't exist" (#7524)

FIXED Email Protection: Fixed restore of Gmail account resulting in error "can't write, error -8260 (MIME data is not valid)" for many files (#7536)

FIXED Email Protection: Reduced time for restoring emails with multiple Gmail labels (#7654)

FIXED Tape Support: Fixed crash when scanning mail slot of Overland Neo T24 library (#7613)

FIXED Configuration Management: Fixed errors with importing localized configurations (#7638)

FIXED Configuration Management: Importing over active configuration no longer results in duplicate volumes (#7639)

FIXED Logging: Moved "NetAddrTop::NetRemember: Duplicate name error" to default log level (#7633)

Console

FIXED Mojave: Fixed localization for operations log error when Retrospect lacks Mojave Full Disk Access (#7631)

FIXED Subscriptions: Status messages are now localized

FIXED Subscriptions: Activities show as failed if license is expired (#7611)

FIXED Activities: Fixed issue with scheduled activities showing up as "Deferred" (#7670) - [See details](#)

FIXED In-App ASM: Fixed issue where expiration date was not displayed for ASM-only licenses (#7500)

FIXED Storage Groups now correctly labeled in Media Sets (#7623)

Client

NEW System Certification for Microsoft Windows 10 October 2018 Update

FIXED Mojave: Fixed issue where "Open Retrospect Client Preferences" menu command did not work (#7620)

Mac 15.5.0.149 – September 4, 2018

Versions

Mac console – 15.5.0.149

Mac engine – 15.5.0.149

Mac client – 15.5.0.145

Windows client – 15.5.0.179

Linux client – 15.1.2.101

Engine

NEW

Management Console Beta - [See details](#)

NEW

Storage Groups Preview - [See details](#)

NEW

Email Global Deduplication - [See details](#)

NEW

Email Local Restore - [See details](#)

NEW

Email Protection for Dovecot - [See details](#)

NEW

System Certification for Microsoft Windows Server 2019

NEW

System Certification for Apple macOS Mojave 10.14

NEW

System Certification for Ubuntu 17.10, 18.04

NEW

System Certification for CentOS 7 Update 4, Update 5

NEW

System Certification for RHEL 7 Update 4, Update 5

NEW

System Certification for SUSE Linux Enterprise 12 SP 3

NEW

LTO-8 "Type M" Certification

FIXED

Email Protection: Fixed "error -8,254 (file not found)" issue ([#7474](#))

FIXED

Configuration Import: Fixed issue with importing client sources ([#7493](#))

FIXED

Client Browsing: Fixed "error 1101" issue with browsing particular folder in macOS High Sierra on client ([#7521](#))

FIXED

Cloud Backup: Fixed "error -1017, expired_auth_token: expired authorization token" error on Backblaze B2 ([#7530](#))

FIXED

ProactiveAI: Fixed -505 error when two ProactiveAI scripts tried to access the same source at the same time ([#7555](#))

FIXED Remote Backup: Fixed issue with getting the default IP address for a remote backup listener (#7470)

FIXED Grooming: Fixed log entry for "Optimizing for performance skipped grooming" to use correct file count (#7503)

FIXED Logging: Increased log level for "soccCallback: kNetSelectorConnect" error to reduce noise (#7480)

FIXED Rebuild: Fixed rare crash during a rebuild (#7506)

Console

FIXED Activities: ProactiveAI activity dates are now "ASAP" if the next activity is now or in the past (#7049)

FIXED Compatibility: Fixed backward compatibility for v15 console and v14 engine (#7573)

Client

FIXED Logging: Fixed crash where log could not write filename with "%" (#7473)

FIXED Logging: Moved packet dump to log level 6 for cleaner logs (#7492)

Mac 15.1.2.101 – June 13, 2018

Versions

Mac console – 15.1.2.101

Mac engine – 15.1.2.101

Mac client – 15.1.0.131

Windows client – 15.1.0.151

Linux client – 15.1.2.101

Engine

FIXED Fixed issue for Windows April 2018 Update where -1103 errors for OneDrive folder prevented system state backup (#7445)

FIXED Fixed cosmetic logging issue for Microsoft SQL using Retrospect configuration import (#7484)

Client

FIXED

Linux Client: Fixed issue with upgrading from v15.0 client (#7485)

Notes

NOTE

Windows Customers: If you are using OneDrive and would like to perform a bare metal

recovery (BMR) on a Windows April 2018 Update system, you need to uncheck the option for "Files On-Demand" during backup. Otherwise, the restore will put a blank folder for your OneDrive data, and that empty folder will be synced to the cloud, erasing any cloud files you may have.

Mac 15.1.1.102 – May 22, 2018

Versions

Mac console – 15.1.1.102

Mac engine – 15.1.1.102

Mac client – 15.1.0.131

Windows client – 15.1.0.151

Linux client – 15.1.0.101

Engine

FIXED

Fixed issue where engine would crash after upgrade when running grooming script with no selector specified (#7465)

Mac 15.1.0.131 – May 17, 2018

Versions

Mac console – 15.1.0.131

Mac engine – 15.1.0.131

Mac client – 15.1.0.131

Windows client – 15.1.0.151

Linux client – 15.1.0.101

Engine

- NEW** Email Migration: Direct Migration using Duplicate Scripts
- NEW** Email Protection: "Restore Entire" option now supported
- NEW** Cloud Protection: path-based S3 API support with v4 signatures
- NEW** Cloud Protection: certification for PCExtreme
- NEW** Cloud Protection: certification for Amazon S3 Canada and One-Region Tier
- NEW** Cloud Protection: certification for Google Cloud Storage Montreal, Netherlands, Mumbai Regions
- NEW** Cloud Protection: certification for Digital Ocean Spaces Singapore
- NEW** Cloud Protection: certification for Aquaray
- NEW** Cloud Protection: certification for Cynnyspace
- NEW** Cloud Protection: certification for on-premise OpenIO
- NEW** Cloud Protection: certification for on-premise SwiftStack
- NEW** Cloud Protection: certification for on-premise Minio including on Synology and QNAP NAS devices
- NEW** Cloud Protection: certification for on-premise Zenko.io including on Synology and QNAP NAS devices
- NEW** Data Retention Policies: file selector support for grooming for GDPR compliance
- NEW** Support for Alto DiskArchive storage devices
- NEW** Support for Windows Spring 2018 Update
- IMPROVED** Cloud Protection: customizable per-URL chunk size now supported in INI file
- IMPROVED** Cloud Protection: customizable per-URL region now supported with "CloudRegion" option in INI file
- IMPROVED** Remote Backup: Engine restart no longer required to enable feature after creating public keys
- IMPROVED** Remote Backup: Client now identifies new server.txt and public key without restart
- IMPROVED** Improved Network Performance for In-App ASM notifications - [See details](#)

IMPROVED Logging: selector name now logged with files selected out of total with every script execution if not default

FIXED Remote Backup: Fixed localized text for error message when "Remote Backup" folder was missing (#7314)

FIXED Email Protection: Fixed a number of localizations (#7186)

FIXED Email Protection: Fixed "TRYCREATE" issue with Zoho account (#7414)

FIXED Email Protection: Fixed Outlook.com "Trouble writing files, error -8255 (file access error)" restore issue (#7294)

FIXED Email Protection: Fixed Outlook.com duplicate folder restore issue (#7297)

FIXED Email Protection: Fixed backup issue where differences between reported size and actual size caused problems (#7300)

FIXED Email Protection: non-ASCII Gmail labels now supported (#7336)

FIXED Email Protection: Fixed issue with "HEADER" error for Exchange mailboxes (#7339)

FIXED Email Protection: Mailboxes with non-ASCII names now supported for subvolumes/favorite folders (#7361)

FIXED Email Protection: Fixed issue with Apple iCloud where scanning did not complete for some mailboxes (#7371)

FIXED Email Notifications: daily backup report email now uses latest backup date (#7409)

FIXED Email Notifications: Fixed CSS issue for displaying emails on iPhone Mail (#6875)

FIXED BackupBot: Standardized wording for ProactiveAI (#7308)

FIXED Fixed issue where Retrospect states member "is not a member of this backup set" due to creation date (#7315)

FIXED Configuration Import/Export: Transfer options for transfer snapshot script now included (#5580)

FIXED Fixed issue where external hard drives are not available with "-1101" error if user logs out then logs in (#6024)

FIXED Operations log now includes media request timeout value (#7072)

FIXED Fixed issue where scanning failed for a NAS share with "error -1011 (API request impossible)" (#7364)

FIXED Fixed issue where scanning failed for a folder name starts with UTF-16 char with low-byte 0

(#7396)

FIXED

Fixed rare crash for scanning volumes on an APFS system (#7426)

Console

IMPROVED

Clarified that "Schedule" button for ProactiveAI is a one-time schedule change

FIXED

"Automatically add clients using public keys" preference was not saved correctly (#6918)

FIXED

Email accounts now correctly identified as IMAP in Sources (#7218)

FIXED

[Mac] UI does not properly display error string for error kErrEmailMailboxNotFound (#7312)

Client

FIXED

Windows Client: Fixed Wake-On-Lan (WOL) for upgraded Windows client (#7358)

FIXED

Mac Client: Fixed issue where client did not prevent macOS from going to sleep during backup (#7273)

FIXED

Mac Client: Fixed localization for Mac client update log error (#7042)

FIXED

Linux Client: Fixed issue where Linux client left `retropds.23` process after operation completed (#7387)

NOTE

Linux Client: In a future update, Linux clients running on server-level Linux distributions will be treated as server clients

NOTE

Mac Client: [Support End-of-Life Announcement for Mac OS X 10.3, 10.4, and 10.5](#)

Mac 15.0.0.190 – March 6, 2018

Versions

Mac console – 15.0.0.190

Mac engine – 15.0.0.190

Mac client – 15.0.0.190

Windows client – 15.0.0.269

Linux client – 15.0.0.103

Engine

- NEW** Email Protection - [See details](#)
- NEW** BackupBot - [See details](#)
- NEW** Remote Backup - [See details](#)
- NEW** Data Hooks - [See details](#)
- NEW** Support for LTO-8 tape devices
- IMPROVED** Email Notifications: Support for unauthenticated accounts
- IMPROVED** Cloud Backup: Support for cloud set members exceeding 16 TB
- IMPROVED** Cloud Backup: Support backup to Amazon Snowball and Snowball Edge
- FIXED** Fixed catalog rebuild issue caused by checking Backblaze B2 account authorization too frequently (#7131)
- FIXED** Fixed backup issue when Backblaze B2 requires re-authorization" (#7115)
- FIXED** Fixed Dropbox backup issue with intermittent "-1010" API request errors (#7092)
- FIXED** Allowed catalog rebuild to continue after skipping invalid backup data that causes error -641 (#7177)
- FIXED** Fixed catalog rebuild for backup set that have been moved to a different volume (#7127)
- FIXED** Full volume backup and copy now exclude backup set content, which can still be backed up or copied using favorite folders (#7212)
- FIXED** Fixed issue where non-English character in volume name prevents backup set creation (#7242)
- FIXED** Removed erroneous Thorough Verification warnings when copying to LTFs tapes (#6866)
- FIXED** Script hooks now fire for both volumes and favorite folders (#7046)
- FIXED** Fixed issue with media request timeout setting not taking effect (#7070)
- FIXED** Changed defaults for "Wake-on-LAN" option: disabled for proactive backup and enabled for other scripts (#7237)

Console

- IMPROVED** Console now automatically adds the local server that is present

IMPROVED Console now automatically launches the server installer when no local server is present

IMPROVED Console now automatically selects the first server on launch

FIXED Fixed German translation in Preferences (#7107)

FIXED Fixed licensing text where "different or more capable license required" meant "Server license required" (#6787)

FIXED Fixed issue where upgrading server while proactive was paused prevented license entry (#6138)

Client

NEW Linux client installer supports multiple public keys

FIXED Fixed Linux client installer errors on Ubuntu and Debian (#7199)

NOTE In a future update, Linux clients running on server-level Linux distributions will be treated as

server clients

FIXED Fixed Wake-on-LAN option for different network topologies (#6477)

Mac 14.6.1.101 – November 13, 2017

Versions

Mac console – 14.6.1.101

Mac engine – 14.6.1.101

Mac client – 14.6.0.127

Windows client – 12.6.0.157

Linux client – 11.0.0.107

Engine

FIXED Fixed issue with cloud backup where Retrospect does not automatically handle route forwarding for Amazon S3 buckets outside the default region (#7064)

Mac 14.6.0.127 – November 7, 2017

Versions

Mac console – 14.6.0.127

Mac engine – 14.6.0.127

Mac client – 14.6.0.127

Windows client – 12.6.0.157

Linux client – 11.0.0.107

Engine

- NEW** Cloud storage support for DigitalOcean Spaces
- NEW** Cloud storage support for Aufiero Informatica
- NEW** Cloud storage support for Google Cloud Storage Frankfurt and São Paulo
- NEW** Support for concurrent backups from different favorites of the same source
- NEW** Customizable HTML email template - [See details](#)
- IMPROVED** Daily backup report enhancements for large-scale environments
- IMPROVED** Improved error reporting for better notifications - [See details](#)
- FIXED** HFS+ volume that is converted to APFS now automatically recognized as original volume (#6993)
- FIXED** Retrospect now excludes APFS swap volume ("VM") under Sources (#6998)
- FIXED** Fixed hang during backup when zero-byte RDB files cause error "Can't write to file, error -1023 (already exists)" (#6936)
- FIXED** Fixed networking issue with finding client after Retrospect's default network interface IP changed (#7022)
- FIXED** Fixed engine crash during certain storage-optimized groom operations (#6939)
- FIXED** Fixed engine crash in storage-optimized groom due to invalid info in catalog (#6976)
- FIXED** Fixed UI issue where cloud backup progress text was incorrect (#6986)
- FIXED** Fixed logging information for Backblaze B2 backups to log relevant information at default log level (#6992)
- FIXED** Updated versions in engine installer receipt (#6963)

FIXED Fixed UI issue with rebuild for Backblaze B2 backup sets using bucketName/subPath (#6996)

Client

FIXED Improved resiliency of client backup during long operations against error -519 (#6938)

FIXED Improved CPU efficiency of certain client operations (#6961)

FIXED Corrected text for client RCU updates (as they do not require an administrator to be logged in) (#6812)

FIXED Updated versions in client installer receipt for mass headless deployment (#6476)

FIXED Fixed client network issue for MacBook Pro with Touch Bar (#6934)

Mac 14.5.0.146 – September 5, 2017

Versions

Mac console – 14.5.0.146

Mac engine – 14.5.0.146

Mac client – 14.5.0.146

Windows client – 12.5.0.177

Linux client – 11.0.0.107

Engine

NEW Support for MySQL database protection via script hook - [See details](#)

NEW Support for PostgreSQL database protection via script hook - [See details](#)

NEW Support for MongoDB database protection via script hook - [See details](#)

NEW System Certification for Apple macOS High Sierra with Apple File System (APFS) - [See details](#)

NEW Daily backup report email - [See details](#)

NEW Cloud storage support for Wasabi

IMPROVED Retrospect Dashboard includes improved media request text

FIXED Fixed rebuild issue where certain block-level incremental backups (BLIB) are incorrectly

excluded from catalog (#6767)

FIXED Updated bundle version numbers for engine and Instant Scan bundles (#6871)

FIXED Fixed issue with Configuration Import where long names or certain characters led to application crash (#6852)

FIXED Fixed issue with Configuration Import where execution units were not set correctly (#6822)

FIXED Fixed crashes related to scalable data protection (#6826, #6831)

Console

FIXED Fixed system log message for "App Transport Security" when launching Console (#6769)

Client

NEW System Certification for Microsoft Windows Fall Creators Update

NEW System Certification for Ubuntu Linux 15, 16, and 17

NEW System Certification for RHEL 7 Update 3

NEW System Certification for CentOS Linux 7 Update 3

NEW System Certification for Suse Linux 11.4 and 12.2

NEW System Certification for Debian Linux 8 and 9

FIXED Fixed client restore issue where suid bit for file and folder was not set correctly (#6837)

FIXED Fixed client workflow for restoring backup from client where the set is in a folder (#6792, #6909)

FIXED Fixed issue where client's History tab failed to populate after engine had been restarted (#6915)

FIXED Fixed issue that prevented script hooks from being executed (#6798)

FIXED Fixed Windows client issue with block-level incremental backup (BLIB) where restore fails for read-only files (#6860)

FIXED Added error for Windows client block-level incremental backup (BLIB) restore where Retrospect fails to find base file (#6850)

Known issues

As of beta 8, Retrospect cannot perform a bootable restore or bootable duplicate for an APFS destination volume. We are working with Apple to resolve this issue.

Mac 14.1.0.138 – June 6, 2017

Versions

Mac console – 14.1.0.138

Mac engine – 14.1.0.138

Mac client – 14.1.0.138

Windows client – 12.1.0.174

Linux client – 11.0.0.107

Engine

- IMPROVED** 50% faster cloud backup for Internet connection above 250 Mbps
- IMPROVED** Local restores now moderately faster with performance optimizations
- IMPROVED** Increased performance of configuration import
- FIXED** Fixed issue with Slack integration where the status incorrectly showed "0 files" (#6754)
- FIXED** Fixed rebuild issue with media set name that starts with a number followed by a dash (#6695)
- FIXED** Fixed groom issue that could cause restore problem if thorough rebuild hasn't been performed prior to groom (#6737)
- FIXED** Fixed storage-optimized groom issue that cause restore problem in some cases for block-level incremental backups (#6701)
- FIXED** Fixed uncommon case of fast rebuild misreporting block-level incremental backup chains as broken and not restorable (#6668)
- FIXED** Fixed -1101 errors when saving fast rebuild cache (.session) files to media sets on network volume with similar name as other network volume (#6720)
- FIXED** Fixed configuration import issue where scripts and clients share the same name (#6489)
- FIXED** Fixed assert in an uncommon case when saving fast rebuild cache file (#6694)

FIXED Fixed assert after rare file IO error (#6732)

FIXED Fixed rare crash when Retrospect set to back up file security information but not folder security information on Windows (#6813)

FIXED Fixed rare crash when accessing Windows Client volume information in Retrospect's configuration (#6667)

FIXED Fixed misreported "error segment data" for multi-member media set (#6725)

Console

IMPROVED Annual Support and Maintenance information integrated into product

Client

NEW Support for Microsoft Windows Creators Update

FIXED Fixed Mac client hooks for external scripting with event handlers (#6750)

FIXED Fixed Windows client issue where the client logs -1101 errors then terminates (#6740)

FIXED Improved logging for multicast IP addresses on Windows clients (#6693)

Known issues

LTFS for Mac support does not copy extended attributes larger than 4096 bytes

Mac 14.0.0.183 – March 7, 2017

Versions

Mac console – 14.0.0.183

Mac engine – 14.0.0.183

Mac client – 14.0.0.183

Windows client – 12.0.0.188

Linux client – 11.0.0.107

Engine

NEW Scalable Data Protection

- NEW** Cloud storage support for Backblaze B2
- NEW** Monitoring System Integration
- NEW** Script Hooks
- NEW** Support for Avid
- NEW** Support for LTFS
- NEW** Support for Quantum Scalar i3–i6 Tape Libraries
- IMPROVED** Performance improvement during backup and restore for computers with more than 500,000 folders
- IMPROVED** Operations log now includes storage savings statistics for block level incremental backup (BLIB)
- IMPROVED** Operations log now supports up to 999MB
- FIXED** Resolved intermittent issue with multiple processes left behind from mounting NAS shares (#6454)
- FIXED** Thorough Catalog Rebuild now correctly deletes previous .session files (#6598)
- FIXED** Grooming policy now correctly saved to backup set to preserve with rebuild (#6549)
- FIXED** Fixed "Scanning incomplete, error -645" error (#6531)
- FIXED** Fixed issue with cloud backup sets seeing a media request after grooming (#6583)
- FIXED** Grooming now automatically runs during a backup when cloud backup set is full (#6280)
- FIXED** Clarified error for backup set format inconsistency (#5627)
- FIXED** Recycling a backup set correctly removes all existing RDB files (#6213)
- FIXED** Fixed issue where auto-cleaning request for tape devices was ignored (#6171)
- FIXED** Fixed Dropbox backup error -1010 by automatically retrying upload (#6524)
- FIXED** Fixed ASR errors for disaster recovery restores of Windows Client (#6395)
- FIXED** Improved media verification for block level incremental backup (BLIB) and Thorough Catalog Rebuild to exclude backups with related errors (#6464)
- FIXED** Fixed crash during matching for certain instances of grooming (#6568)
- FIXED** Resolved grooming issue when .session file is manually deleted (#6467)
- FIXED** Fixed issue with importing Retrospect configuration XML with duplicate names for script

sources (#6493)

FIXED File backup and restore errors are now counted as execution errors instead of warnings (#6525)

FIXED Fixed repeated error log entries for "Grx::grxSearchForPartialFiles: can not find node path" for grooming (#6614)

FIXED Backup set transfers with the recycle option enabled no longer log a message saying "Manual recycle" (#6571)

FIXED Support macOS's network interface order (#6313)

FIXED Fixed issue with restoring file name containing the "ö" character (#6573)

Console

NEW Export backup report for server using "Export Backup Report" in Preferences > General

IMPROVED Customers with expiring trial licenses now see a message in the app and receive an email

FIXED Resolved issue with "Check for Updates" on macOS Sierra (#6491)

FIXED Fixed French localization error for storage-optimized grooming (#6506)

FIXED Fixed localization error "Access Denied" error for cloud backup sets (#6615)

FIXED Cloud backup sets can now change their "Use at most" value (#6526)

Client

IMPROVED Network connectivity

IMPROVED Updated SMART status reporting for macOS 10.11 and higher

FIXED Fixed issue where client continued to run after script ended (#5621)

FIXED Clients not found on the network correctly reported as -530 instead of -519 (#6080)

FIXED Client support macOS's network interface order (#6313)

FIXED Client correctly respawns after any crash (#6432)

Known issues

LTFS for Mac support does not copy extended attributes larger than 4096 bytes

Mac 13.5.0.173 – September 14, 2016

Versions

Mac console – 13.5.0.173

Mac engine – 13.5.0.173

Mac client – 13.5.0.173

Windows client – 11.5.0.190

Linux client – 11.0.0.107

Engine

NEW

Cloud storage support for Dropbox - [See details](#)

NEW

Server configuration management - Import and export Retrospect's configuration, including cross-platform support - [See details](#)

NEW

Certified for macOS Sierra (pending final OS release)

IMPROVED

Create cloud storage locations (buckets) directly within Retrospect instead of using third-party tools

IMPROVED

Increased grooming's maximum number of backups to keep to 999

IMPROVED

Dramatically reduced storage footprint by up to 90% for backup metadata on media when using compression

FIXED

Fixed issue with configuration import for client and backup set with the same name (#5532)

FIXED

Fixed issue with configuration import for Linux clients (#5499)

FIXED

Fixed issue with configuration import for client network interfaces (#5703)

FIXED

Fixed issue with configuration import for script options saying "Provided login information incomplete" (#5528)

FIXED

Fixed provider.cpp assertion failure when importing configuration in certain cases (#6361)

FIXED

Excluded compare errors for /Library, ~/Library and /private (#6136)

FIXED

Fixed issue with block-level incremental backup (BLIB) when two backups have the same timestamp (#6137)

FIXED

SMTP errors now logged correctly (#6133)

FIXED

Fixed rare licensing issue where engine needed to be relaunched for backups to run (#6363)

- FIXED** Apply Software Compression option to Microsoft Outlook PST files (#6249)
- FIXED** Fixed issue where performance grooming could not be selected in certain instances (#6085)
- FIXED** Repairing a media set now correctly uses fast catalog rebuild (#6285)
- FIXED** Fixed errors for lost public/private key pair from "Error -1" to "Error -560" (#6153)
- FIXED** Fixed issue with fast catalog rebuild where cached data is not correctly updated in some cases (#6303)
- FIXED** Fixed issue with grooming when fast catalog rebuild's cached data is not up-to-date (#6302)
- FIXED** Fixed fast catalog rebuild to handle previously failed groom to prevent data integrity issues (#6161)
- FIXED** Log location of newly added cloud backup set member (#5956)
- FIXED** Improved block-level incremental backup (BLIB) performance issue when large number of files matched prior backups (#6233)
- FIXED** Retry access to cloud set member up to ten times in case of temporary network errors (#6300)

Console

- FIXED** Fixed syncing error when a media set member was offline (#6254)
- FIXED** Groom scripts are now able to select cloud sets for scripted grooming (#6170)

Clients

- NEW** Windows: Certified for Microsoft Windows 10 Anniversary Update
- NEW** Windows: Certified for Microsoft Windows Server 2016 (pending final OS release)
- NEW** Windows: Certified for Microsoft Windows Server Core 2008 R2, 2012, 2016 (pending final OS release)
- FIXED** Mac: Reduced frequency for the error message "Unable to bind to valid boot port" (#5202)

Known issues with this release

Network disconnection during cloud restore results in many -1107 errors.

Mac 13.0.1.106 – April 12, 2016

Versions

Mac console – 13.0.1.106

Mac engine – 13.0.1.106

Mac client – 13.0.1.104

Windows client – 11.0.0.252.2

Linux client – 11.0.0.107

Engine

NEW

Cloud storage support for Amazon S3 Frankfurt and Amazon S3 Seoul

NEW

Cloud storage support for Amazon S3 Infrequent Access, Reduced Redundancy, and Glacier - [See details](#)

NEW

Cloud storage support for Google Cloud Storage Durable Reduced Availability and Nearline - [See details](#)

IMPROVED

Log now reports what type of grooming is used: storage-optimized or performance-optimized (#6086)

FIXED

Fixed issue with Mac clients not displaying volumes after logout and login (#6122)

FIXED

Fixed crash when storage becomes full during backup and grooming starts (#6107)

FIXED

Fixed data issues when a v11 set is groomed in earlier release then rebuilt in v11 again (#6119)

FIXED

Fixed support for Japanese characters in cloud backup sets (#6028)

FIXED

Fixed support for non-ASCII characters in cloud backup sets for certain storage providers (#6096)

FIXED

"Restore Bandwidth" limit for cloud backup now respected (#5917)

FIXED

Fixed issue where two cloud backups can temporarily exceed bandwidth limit (#5879)

FIXED

Fixed cosmetic issue where grooming operation reports incorrect size as capacity (#6079)

FIXED

Fixed issue where a restore that included block-level incremental backup files displayed a remaining size (#6105)

FIXED

Fixed network logging for email notifications (#6133)

FIXED

Fixed issue where clients not found on network incorrectly reported as error -519 instead of -530 (#6080)

Console

FIXED Fixed UI issue where a cloud backup set's secret key was not hidden (#6116)

FIXED Fixed UI issue in French where button did not show full text (#6089)

FIXED Fixed UI issue in German where text fields incorrectly overlapped (#6140)

Clients

FIXED Fixed issue with Mac clients where backup process is not correctly cleaned up after completion (#6148)

FIXED Fixed Windows client installer hang during certain scenarios on Windows 10 (#6108)

Known issues with this release

Network disconnection during cloud restore results in many -1107 errors.

Mac 13.0.0.230 – March 1, 2016

Versions

Mac console – 13.0.0.230

Mac engine – 13.0.0.230

Mac client – 13.0.0.230

Windows client – 11.0.0.252

Linux client – 11.0.0.107

Engine

NEW Cloud backup

NEW Performance-optimized grooming

NEW Faster Catalog Rebuild

IMPROVED Backup and restore performance improvements

IMPROVED Added log message for live restores on OS X El Capitan due to new System Integrity Protection

- IMPROVED** Media sets are now able to be easily moved to another location
- IMPROVED** Now supports simultaneous access to different sets on the same volume
- IMPROVED** Faster matching for Windows backup source with lots of root/first level and second level folders
- IMPROVED** "Building Snapshot" performance optimizations for Windows backup source with 150,000+ folders
- FIXED** Fixed resiliency issues if Retrospect loses connection to media set on network share (#5357)
- FIXED** Fixed media request issue if Retrospect loses then regains connection to media set on network share (#5753)
- FIXED** Fixed hang when Retrospect encounters device error when writing to media set (#5620)
- FIXED** Fixed restore issue when large files are moved between block-level incremental backups (#5435)
- FIXED** Fixed grooming issue where log displays "header count invalid" and "make count invalid" (#5400)
- FIXED** Reduced snapshot size when backing up a Windows 2012r2 server with data deduplication enabled (#5579)
- FIXED** Fixed cross-platform restore for larges files with block-level incremental backup enabled (#5688)
- FIXED** Fixed missing files when running a Copy Media Set or Copy Backup script under certain scenarios (#2336)
- FIXED** Fixed "Bad Media Set Header" errors in some cases for restore, copying media set and copying backup (#5662)

Console

- FIXED** Fixed launch issue where "Loading Dashboard..." would not disappear (#5698)
- FIXED** Fixed installer issue where client installers and updaters were not correctly placed into folders in /Applications/Retrospect (#5613)
- FIXED** Switched download URL used by software update to HTTPS (#6057)

Client

IMPROVED Linux: added "--silent" switch to client install script

FIXED Menu bar correctly displays immediately after install on OS X El Capitan (#5605)

Known issues with this release

Amazon S3 Frankfurt and Amazon S3 Seoul are not supported at this time.

Cloud set names do not support non-ASCII characters at this time.

Performance-optimized grooming can report incorrect number of files groomed out.

Network disconnection during cloud restore results in many 1107 errors.

Mac clients on OS X El Capitan report error 1101 when browsed if user logs out and logs back in.

12.5.0.111 – September 15, 2015

Versions

Mac console – 12.5.0.111

Mac engine – 12.5.0.111

Mac client – 12.5.0.111

Windows client – 10.5.0.110

Linux client – 10.5.0.103

Engine

NEW OS X El Capitan (10.11) support (pending final OS release)

FIXED Fix hang when client disconnects from network at certain phases of an operation (#5502)

FIXED Fix hang when restoring more than 65,510 folders to a Windows client (#5569)

FIXED Fix crash when restoring Windows client's system state where VSS writer XML data exceeds 32KB (#5570)

FIXED Fix crash when encountering "-559" error during certain phases of Windows client restore (#5571)

FIXED Support catalog rebuild for incorrectly encrypted sets created with Retrospect 10.0.2 for Windows (#5551)

FIXED Backup properties correctly identifies Windows 8.1 Client (#5185)

FIXED Backup properties correctly identifies Windows 10 Client (#5535)

Console

FIXED Dashboard no longer has visual artifacts when scrolling (#4355)

FIXED Media set tape drive binding selection correctly saved after reboot (#4946)

FIXED Fix issue where Copy Backup script transferred same backup multiple times under certain settings (#5524)

Client

NEW Windows 10 support for clients

FIXED Windows client installer correctly finishes on Windows 10 on all systems (#5584)

FIXED Fix issue where Mac client's "Reset password" button didn't update the password under certain conditions (#5538)

FIXED Fix Mac client "-559" errors in a number of workflows (#5575)

FIXED Linux client now correctly handles certain file-level errors during full-volume restores (#4818)

FIXED Linux client now correctly handles certain file-level errors during backup (#4998)

FIXED Linux client installer no longer asks for password when using public/private keypairs (#5505)

12.0.2.116 – June 9, 2015

Versions

Mac console – 12.0.2.116

Mac engine – 12.0.2.116

Mac client – 12.0.2.116

Windows client – 10.0.2.119

Linux client – 10.0.2.104

Engine

- IMPROVED** Building snapshot significantly faster for Windows clients in more scenarios
- IMPROVED** Scanning phase significantly faster in more scenarios (#5434)
- FIXED** Engine and Instant Scan bundles correctly signed for OS X GateKeeper and Firewall (#5363)
- FIXED** Fixed connectivity issues during backup if Retrospect loses connection with media set on network share (#5106)
- FIXED** Restored support for rebuilding media sets from Retrospect for Mac v6.1 (#5367)
- FIXED** Fixed assert for "Copy Media Set" from a rebuilt v6.1 set (#5395)
- FIXED** Fixed memory leak in engine when automatically exporting/importing configuration (#5478)
- FIXED** Fixed -2242 error in grooming for large sets (#5219)
- FIXED** Fixed corrupted restore of block level incremental backup file when disabling "Restore security information" for Windows volume (#5253)
- FIXED** Fixed tape device issue which prevented dragging tape from drive to library slot (#5284)
- FIXED** Fixed Instant Scan issue preventing engine from using older version of Instant Scan on Mac client (#5431)
- FIXED** Treat open file errors (-1020, -1100, -1101 and -1111) as warnings and consolidate in log after twenty entries (#5381)
- FIXED** Fixed -1101 errors for Windows VSS-related "T-32: VssWSetCompResult" file operations (#5342)
- FIXED** Fixed issue when transferring backups from multiple media sets where some files aren't transferred correctly if a set member is marked as missing (#5414)
- FIXED** Fixed issue with Backup on Demand for Mac client that prevents backup in certain scenarios (#5482)
- FIXED** Fixed -516 error when backing up Mac client with private/excluded folders (#5383)
- FIXED** Fixed XML configuration import for subnets (#5326)
- FIXED** Fixed XML configuration import for security preferences (#5327)
- FIXED** Fixed XML configuration import for client volumes and subvolumes (#5316)

FIXED Fixed XML configuration import for proactive backup schedule (#5321)

Console

IMPROVED Sources: use "Locate" for network shares to update network location

IMPROVED Email: success emails do not require failure emails be enabled

IMPROVED Specific errors now included when source unavailable or in use

FIXED Media set total capacity lists correct values (#5247)

FIXED Media Set available capacity lists correct values (#5370)

FIXED Media set summary lists correct "Backups" value after groom (#2648)

FIXED Operations log reports consistent sizes when grooming (#5240)

FIXED Operations log reports consistent sizes on backups after grooming (#5330)

FIXED Fixed UI issue in Media Sets where Remove dialog would not disappear (#5305)

FIXED Operations log formats information correctly during Rebuild or Repair operations in Japanese (#5341)

FIXED Fixed certain workflows where console with multiple engines connected would display incorrect content (#5450)

FIXED "Desktop 5–User Upgrade" license now correctly displays (#5371)

FIXED Mac Client's file system displayed consistently (#5387)

FIXED Fixed reporting issue where reports lost settings under certain scenarios (#5437)

FIXED Fixed window title in "Browse Backup" window in certain workflows (#5423)

FIXED Fixed auto-update workflow for upgrades (#5427)

Client

NEW Linux client support for Retrospect public/private keypairs

IMPROVED Windows clients support sleep and shutdown after backup

FIXED Fixed security issue in client password hash on Mac, Windows, Linux clients (#5469 / CVE-2015-2864) - [See details](#)

FIXED Mac client bundle correctly signed after first launch using Retrospect public/private

keypairs (#5446)

FIXED Linux client clock offset now consistently accurate (#5398)

FIXED Windows clients should not display tape backups in History tab (#5391)

FIXED Fixed a condition that crashes and disables Instant Scan on Windows clients (#5428)

Known issues with this release

Engine: configs.xml, which replaced Config80.bak for speed and robustness, does not import Linux client (#5499). Workaround: re-add Linux clients.

Windows 10 support:

Client installer may hang (#5584)

Backup properties list OS as "Windows 8" (#5535)

12.0.1.104 – April 21, 2015

Versions

Mac console – 12.0.1.104

Mac engine – 12.0.1.104

Mac client – 12.0.0.213

Windows client – 10.0.0.212

Linux client – 10.0.0.114

Engine

FIXED Fix for -1101 scanning errors (#5323)

FIXED Fix for unrestorable files from Copy Backup that consolidates multiple BLIB-enabled sets (#5329)

FIXED Fix for Copy Backup failing to transfer all necessary BLIB data under certain conditions (#5296)

FIXED French log for building snapshot no longer includes Spanish (#5375)

Client

FIXED Mac client uninstaller now removes retroclient.state (#5332)

Known issues with this release

Engine: configs.xml, which replaced Config80.bak for speed and robustness, does not import all settings including client volumes and network subnets (#5316)

12.0.0.213 – March 17, 2015

Versions

Mac console – 12.0.0.213

Mac engine – 12.0.0.213

Mac client – 12.0.0.213

Windows client – 10.0.0.212

Linux client – 10.0.0.114

Engine

- IMPROVED** Performance increases for backup and restore, up to 100% faster - [See details](#)
- IMPROVED** Performance increases for grooming, up to 200% faster - [See details](#)
- IMPROVED** Performance increases for copying backup - [See details](#)
- IMPROVED** Email summaries for high-level details - [See details](#)
- IMPROVED** Email subjects format now "Script name - 2 errors, 3 warnings - Retrospect" for quick evaluation
- IMPROVED** Standardized timestamps in Operations Log and Activity Logs
- IMPROVED** Log excluded paths (except Client's private files/folders) at Engine level 5
- FIXED** Suppress Finder dialog on remote computer when adding network share (#5018)
- FIXED** Fix performance for slow "Building snapshot" when backing up Windows EFI Clients (#4889)
- FIXED** Folders named "Retrospect" (aside from disk set folders) are now correctly backed up (#5129)
- FIXED** Fix hang during Mac client backup with corrupted file (#5008)
- FIXED** Rebuild correctly handles recycled disk set with existing backup date (#5159)

- FIXED** Fix for an edge case where grooming a set with BLIB files results in an unrestoreable file (#5194)
- FIXED** Fix for periodic unresponsive engine when autosaving very large config DAT file (#5302)
- FIXED** Changing the media set "Use at most" option when backing up to a NAS no longer results in a media request (#3861)
- FIXED** Better warning for hard-linked directories (like Time Machine) (#4919)
- FIXED** Repair catalog of media set with members on different disks doesn't use specified member (#5215)
- FIXED** Add progress bar and relevant log entries for building snapshot (#5050)
- FIXED** Add progress bar and relevant log entries for catalog repair (#5149)
- FIXED** Add progress bar and relevant log entries for restore (#5165)
- FIXED** Fix for using certain NAS devices as destination (#5137)
- FIXED** Report VSS writer and component (MetalInfo) backup errors on 64-bit Windows client (#4968)

Console

- NEW** Dashboard hover window for detailed at-a-glance backup information - [See details](#)
- IMPROVED** Copy Backup script's transfer mode now included in "Summary" tab
- IMPROVED** Email SSL option makes secure SMTP connection explicit to avoid insecure previous SSL to non-SSL fallback - [See details](#)
- IMPROVED** "Add Share" buttons available in "Add Member" sheets
- NEW** Grooming "Months to keep" setting - [See details](#)
- NEW** Instant Scan checkbox for enabling or disabling service on clients - [See details](#)
- FIXED** Operations log includes full file name for rebuild activity that contain missing files (#3265)
- FIXED** "Source Host" rule fixed in French (#3348)
- FIXED** App remains responsive during catalog rebuild operations (#3857)
- FIXED** Operations log and activity logs now correctly contain warning, error, set, folder, license icons (#3859)
- FIXED** "Disable restore" checkbox for client no longer prevents RCU updates on that client (#4129)

- FIXED** Console better handles engine going offline (#3869)
- FIXED** Fix "Tape Bindings" selection not being saved (#4946)
- FIXED** Fix for past backups not showing up immediately in certain cases (#5014)
- FIXED** Fix for Copy Backup script's transfer mode not being saved in certain workflows (#5037)
- FIXED** Fix for Copy script's transfer mode not being saved in certain workflows (#5042)
- FIXED** Backups not listed under Restore Assistant or Scripts after engine restarted (#5243)
- FIXED** Fix for past backups incorrectly listing zero files in certain cases (#5044)
- FIXED** Fix "Locate" button for clients after an engine restart (#4859)
- FIXED** Fix for scheduling error handling the last day of the month (#4994)
- FIXED** Fix for on-demand options resetting under certain conditions (#4521)
- FIXED** Console should highlight password field for update password (#5261)
- FIXED** Fix console crash after engine removed while connecting (#5244)

Client

- IMPROVED** Native 64-bit Linux support - [See details](#)
- FIXED** Support for Linux v7.7 clients (#5003)
- FIXED** Handle Japanese backup set names in Windows client (#4046)
- FIXED** Fix for empty History tab on Windows client (#3068)
- FIXED** Fix for backing up Mac client volumes with paths over 1024 characters that could cause incomplete backups (#5139)
- FIXED** Adding volumes to Privacy pane no longer crashes UI on OS X 10.6 (#5009)
- FIXED** Fix Mac client crash during restore in certain conditions (#4437)

Network

- NEW** "Ignore client discovery" checkbox for preserving Client's address in certain firewall and NAT environments
- FIXED** Fix security issue where password sent in cleartext when engine setting password on passwordless client (#4786)
- FIXED** Better handle multi-NIC environments for on-demand client operations (#4875)

- FIXED** Better handle change for Engine's NIC for on-demand client operations (#4858)
- FIXED** Fix hang when client machine disconnected from network during backup (#5054)
- FIXED** Better handles network address changes (#4952)
- FIXED** Offline network shares time out quickly (#3618)
- FIXED** Fix intermittent issue where client connection reverted to older IP address (#5027)

11.5.3.103 – December 22, 2014

Versions

Mac console – 11.5.3.103

Mac engine – 11.5.3.103

Mac client – 11.5.2.104

Windows client – 9.5.0.139.3

Linux client – 9.5.0.113

Console

- FIXED** Corrected performance issue for very large environments (#5098)
- FIXED** Sources: Tags field in "Summary" no longer shows duplicate tags (#5089)
- FIXED** Sources: Tag name no longer remains in "Summary" after it is removed from the source (#5090)
- FIXED** Past Backups: "Save" button stays in correct location when the "Browse" window is resized (#5096)
- FIXED** Backup Assistant: Block Level Incremental Backup checkbox stays in correct location when the window resized (5093)
- FIXED** Backup/Copy Assistants: Browse and Preview no longer automatically switch the saved rule to "Manual File Selection" (#5094)
- FIXED** Scripts: "Activity Thread" setting was not saved after clicking "Save" in certain scenarios (#5099)
- FIXED** Scripts: Copy script warning updated to "Warning: Destination's contents will be replaced" for clarity (#5095)
- FIXED** Dashboard: fix French translation (#5088)

Engine

FIXED "Copy Media Set" now includes all snapshots including those not retrieved (#5082)

FIXED Fix grooming issue where in complex scenarios grooming could corrupt files backed up with BLIB (#5116)

FIXED Fix grooming and set copy issue where certain scenarios could restore corrupted versions of files backed up with BLIB (#5109)

Known issues with this release

Engine: Customers can encounter the following message in the log during grooming:
"grxSearchForPartialFiles: unable to find all dependent partial files for 'file_path'". For large files using Block Level Incremental Backup (BLIB), this indicates that older versions of the file have been groomed out by prior Retrospect releases and are no longer restorable (#5085), but the most recent full/base version and the incremental versions based on it are properly preserved. For files not using BLIB, these messages can be safely ignored, including backups from SQL and Exchange add-ons (#5100).

11.5.2.104 – October 31, 2014

Versions

Mac console – 11.5.2.104

Mac engine – 11.5.2.104

Mac client – 11.5.2.104

Windows client – 9.5.0.139.3

Linux client – 9.5.0.113

General

IMPROVED Full support for OS X Yosemite 10.10

Instant Scan

FIXED Mac version correctly no longer runs in background after upgrade when disabled (#4978)

FIXED Handles Core Storage Logical Volume disk changes on OS X Yosemite (#5002)

FIXED Fix file change scanning when Instant Scan out of date (#4989)

Engine

FIXED Fix issue where client volumes showed up as local volumes under certain workflows (#4995)

FIXED Fix crash on OS X Yosemite for SATA drives connected using certain PCIe cards (#5010)

11.5.1.104 – September 23, 2014

Versions

Mac console – 11.5.1.104

Mac engine – 11.5.1.104

Mac client – 11.5.0.137

Windows client – 9.5.0.139.3

Linux client – 9.5.0.113

Engine

IMPROVED Support for GateKeeper on OS X Yosemite 10.10 and OS X Mavericks 10.9.5

FIXED Fix "Error -517" during restores to Windows client (4915)

FIXED Fix backup for Mac folder ACLs under certain scenarios (#4922)

FIXED Fix folder ACLs on Windows EFI client restore with system state (#4927); doesn't affect back up

FIXED Fix "osErr 305, error -1001" when restoring to Windows Client with short file name disabled (#4072)

FIXED Fix Windows Client update "error -1" failures under certain conditions on x86 systems (#4929)

FIXED Windows 8.1 EFI Client's Metro tiles now correctly show up after system state restore (#4724)

FIXED Fix wrapper1.cpp-5678 assertion failure during local (non-Client) system state restore (#4941)

FIXED Fix error -517 when restoring to Windows Client's favorite folder (#4915)

11.5.0.139 – September 9, 2014

Versions

Mac console – 11.5.0.139

Mac engine – 11.5.0.139

Mac client – 11.5.0.137

Windows client – 9.5.0.139

Linux client – 9.5.0.113

Engine

FIXED Fix engine assertion error soccon.cpp-491 when accessing clients (#4033)

FIXED Report errors but continue to groom to free disk space instead of aborting on data errors (#4892)

FIXED Fix slow restore that occurs in some cases when using Retrospect 11 (#4775)

FIXED Update progress when reading and skipping unmodified file blocks during Block Level Incremental Backup (BLIB) (#4209)

FIXED Exclude compressed files (pptx, xlsx, docx, zip) from BLIB (#4515)

FIXED Exclude known compressed file types from built-in compression algorithm (#4734)

FIXED Fix error -523 for BLIB which is unsupported but enabled for Mac client 6.3 (#4586)

FIXED Closing network connection hang in certain conditions (#4730)

Console

IMPROVED Significant performance improvements when connected to remote engines

NEW Export backup list to CSV file from Past Backups when browsing backup

IMPROVED Reduced download by 200MB with single Windows client installer for all languages

FIXED Crashes when engine quits (#4491)

FIXED Dashboard displays backups based on Activities and Past Backups (#4426)

FIXED Past Backups performance improvements for large installations (#4662)

FIXED Past Backups: "Remove" dialog no longer hangs when removing many backups (#2954)

FIXED Past Backups: all toolbar searches correctly saved (#4684)

- FIXED** Media Sets: Groom/Recycle buttons available immediately after unlocking set (#2902)
- FIXED** Media Sets: "Free Space" displays as 0 when first member marked 'Lost' (#2106)
- FIXED** Save DNS name instead of IP for servers (#4665)
- FIXED** Error handling when server quits (#4681)
- FIXED** Update client errors to match knowledgebase (#4768)
- FIXED** Show error when network unavailable during client discovery (#4770)
- FIXED** Scripts: Copy Media Set script only supported "All Files" rule (#3021)
- FIXED** Scripts: remove legacy Countdown settings from Proactive Backup options (#4529)
- FIXED** Scripts: remove legacy Disconnect message from Proactive/Backup Options (#4710)
- FIXED** Scripts: fixed schedule days in all languages (#4685)
- FIXED** Sources: error during "Refresh" displays alert (#4767)
- FIXED** Activities: scripts incorrectly display as "Utility" temporarily (#4640)
- FIXED** Restore Assistant "Search for Files": search displays progress (#4756)
- FIXED** Restore Assistant "Search for Files": search displays files/size for found sets (#4750)
- FIXED** Restore Assistant "Search for Files": Browse Backup lists set name for clarity (#4748)
- FIXED** Restore Assistant "Search for Files": "Cancel" stops search (#4757)
- FIXED** Restore Assistant "Search for files": easily allow "All" or "None" selection in search (#3846)
- FIXED** Restore Assistant "Search for Files": highlight only first found set (#4747)
- FIXED** Restore Assistant "Search for Files": second search no longer lists previously found sets (#4749)
- FIXED** Restore Assistant "Search for Files": including locked set in search prompts for unlock (#4755)
- FIXED** Logs sometimes display incorrect information (#4500)
- FIXED** Quick Look app now localized to all supported languages (#4524)

Email

- FIXED** Engine hangs in some cases at end of backup when sending email notification (#4619)
- FIXED** "Email notification failed: error -530 (backup client not found)" is "Email notification failed:

error -593 (invalid server address)" (#4386)

FIXED Show "SMTP server requires authentication" instead of incorrect "invalid email address" (#3717)

FIXED Support recent Gmail SMTP changes (#4819)

FIXED Support sending emails containing non-ASCII characters as secured email (#4812)

Client

NEW Added support for "-ipsave"

IMPROVED Linux: "Building snapshot..." significantly faster

IMPROVED Linux: added support for recent distros - [See details](#)

FIXED Fix mac client crashing when restoring meta data (#4723)

11.0.1.110 – March 27, 2014

Engine

FIXED Move more block level incremental backup logging into debug logging (#4494)

FIXED Restore issue for file with block level incremental backup enabled on two members with first marked missing (#4552)

FIXED Restore issue from a backup with no file changes transferred set with block level incremental backup enabled (#4357)

FIXED Copy backup script failure with recycle enabled for source and destination (#4557)

FIXED Restore of the 32nd block level incremental backup of a file fails if it is unchanged since the prior (31st) backup (#4499)

FIXED Restore issue with block level incremental backup set after rebuild (#4558)

FIXED Memory leak during grooming (#4527)

FIXED Compare issue with thorough verify during block level incremental backup of local NTFS files with OBJECT_ID stream (#4497)

FIXED Cosmetic issue in log where it shows negative files for block level incremental backup under certain circumstances (#4508)

FIXED Restore issue with ACLs on root volume (#4589)

Console

FIXED More intermittent cases of Past Backups not refreshing (#4592)

FIXED Past Backups view still showed removed backups (#4476)

FIXED Past Backups view did not show retrieved backups (#4512)

FIXED Dashboard information was not accurate on OS X 10.9 on Japanese under certain circumstances (#4368)

FIXED Dashboard "Sources" translation corrected in French (#4567)

FIXED Dashboard no longer flashes OK button after engine upgrade (#4431)

11.0.0.194 – March 4, 2014

Engine

NEW Block level incremental backup - [See details](#)

FIXED Fix engine assertion errors (netcotop.cpp-427, soccon.cpp-491) during network backup (#4018)

FIXED Fix engine assertion error when connected with Retrospect Touch for iOS (#2703)

FIXED Copy script to Mac volume didn't reliably set destination folder's creation and modification dates (#4240)

Email

NEW Enhanced email reporting with logs included for easy filtering

NEW Option to send e-mail on server startup or shutdown

IMPROVED Consolidate emails into one email per backup source for Proactive script and one email per script for other script types

IMPROVED Send email notification for each repeated script execution, while still limiting emails for certain warnings to once a day

FIXED Disabling the "Send e-mail for failure and media requests" option now automatically disable other e-mail options (#4237)

Console

- NEW** High-level dashboard
- FIXED** Fix several intermittent cases of Past Backups not refreshing (#3719)
- IMPROVED** Allow manually changing order of backup sources in scripts
- FIXED** Correctly display server-specific changes (e.g. in Scripts) when connected to multiple servers (#3943)
- FIXED** Fix Copy Backup script's drop down from reverting to "Copy most recent backups for each source" when reopening console (#4115)
- IMPROVED** Add new Path column for Backup script under Sources, in case there are different Favorites with the same name (#3843)
- FIXED** Allow sorting of media sets that are in Busy state (#1176)
- FIXED** Disable Run button when script is modified but not saved (#4173)
- FIXED** Clarify error messages for incorrect licenses (#2860)
- FIXED** Disable Add/Edit Member buttons for locked sets (#3169)
- FIXED** Local favorite folders now include volume name (#3640)
- FIXED** Days of the week corrected in German, French, Italian in Scripts > Schedule (#3990)
- IMPROVED** Installer for server and client list version
- IMPROVED** Console displays "Upgrade local server" when older local server present
- IMPROVED** Console auto-selects first syncing server
- IMPROVED** ASM licenses accepted in License Manager

Known issues with this release

Engine: under some circumstances log shows negative file count for block level incremental backup, even though files are correctly backed up and are restorable (#4508).

Engine: restoring the 32nd block level incremental backup of a large file fails if it is unchanged since the prior (31st) backup (#4499). Workaround: restore from the 31st backup.

Engine: if a backup contains no new/modified files and the backup is transferred, restoring that backup from the transfer destination backup set fails (#4357). Workaround: restore from the source backup set or from prior backup.

Console: Past Backups view show removed backups (#4476). Workaround: restart console.

Console: Past Backups view does not show retrieved backups (#4512). Workaround: restart console.
Console: Dashboard doesn't show all recent backups unless media sets have grooming enabled.
Workaround: retrieve relevant backups or enable media set grooming.
Console: Dashboard information not accurate on OS X 10.9 on Japanese under certain circumstances (#4368). Workaround: switch to 24-hour time.
Console: Dashboard intermittently shows OK button (#4431). Workaround: restart console.

10.5.0.145 – September 19, 2013

General

IMPROVED OS X Mavericks ready — OS X Mavericks 10.9 is fully supported in this version (pending final release).

Engine

IMPROVED Performance boost — This version includes significant performance increases, up to 100% depending on your usage.

FIXED Fix db.cpp-170 assertion failure after upgrading Retrospect (#3945)

FIXED Fix soccon.cpp-491 assertion failure when accessing clients (#4033)

Email

FIXED Fix date and time in email header (#3961)

FIXED Correctly report error if timeout occurs while sending test email (#3875)

FIXED Correct daylight saving time interaction with time zone (#3345)

FIXED Avoid error -511 in log if email is sent successfully using different methods (#3926)

FIXED Fix line breaks in email sent via Apple mail servers (#3349)

FIXED Use consistent subject for email notifications (#3970)

Console

FIXED Tags for client volumes and favorites now correctly selected after re-opening Console (#2347)

FIXED Past Backups not always immediately updated after backup (#3719)

IMPROVED Execution duration and performance now track day change

IMPROVED Ensure Console fits on MacBook Air screen with dock showing

10.2.0.201 – July 10, 2013

Email

IMPROVED Improve compatibility with email servers when sending notification email

IMPROVED Improve support for email notifications with multiple recipients separated by space, comma and semicolon

FIXED Reduce similar email notifications during 24-hour period (#2122)

Console

FIXED Fix manual file selection for Backup and Copy assistants (#3692)

FIXED Fix frequent "spinning pinwheel" and unresponsiveness during backup (#3798)

IMPROVED Add icons in operation log to make it easier to read for troubleshooting

IMPROVED Indicate which portion of operation log is displayed

FIXED Fix formatting of operation log to make it easier to read for troubleshooting (#3790)

IMPROVED Show engine version when prompting for license code

FIXED Fix "Export server installer" for Mac OS X 10.6 (#3845)

Grooming

FIXED Grooming crash left catalog in corrupted state - error 2241 (#3397)

Engine

FIXED Copy script now delete source folders if the "Move files" option is selected (#117)

IMPROVED Building snapshot of Mac clients connected over WiFi sped up from hours to minutes

FIXED Fix compatibility with Retrospect Client 9.x running on Mac OS X 10.5 (#3699)

FIXED Fixed issue with multiple network shares (#3726)

IMPROVED Improve compatibility with Mac OS X 10.8 when mounting AFP network share

IMPROVED Upon assertion failure, flush log entries of on-going activities to operation log

FIXED Fix crash when restoring files with corrupted extended attribute length (#3770)

NEW Support Oracle StorageTek SL 150 Modular Tape Library

Instant Scan

FIXED Fix a case where Instant Scan may crash when Mac OS is starting up, but backup still works correctly (#3638)

10.1.0.221 – March 19, 2013

IMPROVED Refreshed user interface — Retrospect for Mac has been updated with better status information and clearer workflows for syncing server information, adding and updating servers, and managing multiple servers.

NEW Retina display support — The Retrospect for Mac console and client take advantage of Apple's Retina displays.

NEW Updated documentation — The Retrospect User's Guide and help systems have been updated for this release. Documentation is now available online to ensure that they remain up-to-date.

FIXED Adding and removing servers no longer causes all of the servers to expand (#1177)

IMPROVED Media set with the "Remember password for scripted access" option now requires password for non-scripted access

IMPROVED Progress spinner is now shown during remote server update

FIXED Password-protected server can now be correctly unlocked without relaunching Retrospect Console (#2636)

NEW Save and Revert buttons now available after changing media set options

FIXED Scripts: scheduled start time is now the next active day if the start time is set in the past (#3023)

FIXED Renamed rule is now shown correctly without relaunching Retrospect Console (#3062)

FIXED The Uninstaller no longer removes *.utx files (operations log, assert log, etc) (#3125)

FIXED Improve Instant Scan efficiency for detecting file system changes on Mac OS 10.6.8 (#3131)

FIXED Instant Scan now detects if user pulls the plug on external drive without using Finder to eject (#3156)

FIXED Stopping and starting the engine no longer causes network shares to remount (#3159)

FIXED Client prepane can include/exclude for backup all folders with names starting or ending

with the option-8 character (#3172)

- IMPROVED** Instant Scan can be disabled using Retrospect or Client prefpane
- FIXED** Fixed a minor Instant Scan memory leak when processing file system changes (#3182)
- FIXED** Fixed Mac Instant Scan assertion failure due to NTFS volumes in Boot Camp or on external drive (#3183)
- FIXED** Fixed a bug that prevented certain public/private keys from being loaded (#3192)
- IMPROVED** Reduced the Instant Scan process' CPU usage
- FIXED** The "StartRetrolSA" setting in retro_isa.ini is now persistent (#3226)
- FIXED** The retro_isa.ini file no longer has read only admin privileges (#3229)
- FIXED** In Console running activity now stays selected when it completes (#3240)
- FIXED** No longer reports misleading -1101 errors during backup (#3241)
- FIXED** Fix the issue of two identical servers appearing in the left sidebar (#3242)
- IMPROVED** Improve Console workflow for first launch with relevant action buttons
- FIXED** Fixed a bug that caused TString crash on Mac OS 10.6.8 with Instant Scan (#3248)
- IMPROVED** Selected activity's log now automatically refreshes
- IMPROVED** Preferences: "Create keypair" now shows progress indicator
- IMPROVED** While loading various server items, Console now lets users interact with the ready ones
- IMPROVED** Changed disk grooming's maximum number of backups to keep to 250
- IMPROVED** Console now automatically shows upgrade dialog once for each new engine release
- IMPROVED** Show "Update password..." button to unlock password-protected server
- IMPROVED** Show relevant action buttons for unlicensed server
- FIXED** Automatically ignore Instant Scan data if it is stale (#3302)
- IMPROVED** Show warning icon for Server and Console version mismatch
- FIXED** Media Sets: changing capacity of existing member now reflected promptly (#3312)
- NEW** Client UI now displays ethernet icon when communicating with server
- NEW** Auto-update dialog now supports "Learn More" for paid upgrades
- IMPROVED** Console now shows "Unsupported" for unsupported server version

NEW

Co-exist with Console version 8.2

NEW

Support Retina (HiDPI) displays

IMPROVED

Console has added limited support for Server version 8.2 and show "Unsupported" where applicable

NEW

Retrospect System Preferences now supports Retina (HiDPI) displays

IMPROVED

Reduced Instant Scan processor usage when creating initial scans for multiple volumes

NEW

Client prepane now supports Retina (HiDPI) displays

IMPROVED

"Retrospect Files" rule now includes .RDB files

FIXED

Sources: Fixed tags for reports and search bar (#3385)

IMPROVED

Sources: Now include "Tags" in Summary view

10.0.1.105 – December 11, 2012

FIXED

Fixed an issue with AES encryption keys that caused !Bad Media Set Header errors during restore and Catalog rebuild (#3261)

FIXED

Fixed an issue that caused an assert (grx.cpp-1076) during grooming or Catalog rebuild (#3275)

FIXED

Public/private keypairs generated with previous versions of Retrospect can now be loaded (#3281)

10.0.0.174 – November 6, 2012

NEW

Instant Scan Technology — Retrospect now pre-scans NTFS and HFS+ volumes connected to the backup server and Retrospect clients, speeding overall backup and restore operations by removing the lengthy volume scan from backup process. This feature employs the USN change journal (for NTFS volumes) and FSEvents (for HFS+ volumes) to predetermine which files have changed since the last backup to a particular Media Set.

NEW

All-new Retrospect Client for Windows — Support for Windows 8 and Windows Server 2012 — On-demand backup and restore — Interactive taskbar icon with notification of backup operations — Network link encryption now employs the strong AES-256 standard — Support for S.M.A.R.T. hard drive error reporting — Updated user interface

NEW

Support for Mac OS 10.8 "Mountain Lion" — Both the Retrospect console application and the Retrospect Client software support Mac OS X 10.8 Mountain Lion and Mac OS X 10.8 Mountain Lion

Server.

- IMPROVED** Added a progress bar during matching when browsing backup contents
- IMPROVED** Docked the dialog: Please Enter the media set password
- FIXED** Fixed a bug where an error that occurred during creating a Media Set could cause activities to become stuck (#1143)
- FIXED** Fixed a bug where script schedules set to start prior to the current time weren't saved properly (#1199)
- FIXED** Utility-type scripts now list properly in Activities instead of showing as "-" (#1248)
- FIXED** Fixed an issue where "@" in file name would cause beachball during browse backup (#1260)
- IMPROVED** Back Up Now / Restore...: script now includes Client's name
- FIXED** Failed erase of a tape no longer shows up as completing successfully in UI and operations log (#1603)
- FIXED** If the Past Backups window is empty, the Retrieve button is no longer grayed out when there are past backups to add (#1660)
- FIXED** Unsupported multi-byte Media Set passwords now correctly report "Wrong password" during creation (#1779)
- FIXED** Connecting an older console/engine to a newer engine prompts to downgrade (#1822)
- IMPROVED** The log is now properly populated with Errors during a backup/copy after Refresh
- FIXED** It's now possible to add multiple shares on the same NAS device to the same Media Set when using the root share folder (#2044)
- FIXED** Preferences: Email always reports 'Test email successful' (#2104)
- FIXED** Retrospect Mac clients can now properly list volumes where the name is one character (#2152)
- FIXED** Replaced "Backup Set" with "Media Set" in the log for Grooming error: -2241 (#2245)
- FIXED** Browse windows now properly display the various symbols that Finder accepts (#2257)
- FIXED** The Locate command now lists Catalogs saved in /Library/Application Support/Retrospect/Catalogs (#2265)
- FIXED** Clients on-demand buttons are grayed out if the features disabled (#2270)
- FIXED** Sources>Add no longer incorrectly populates the list with sources from multiple Retrospect servers (#2348)

- FIXED** Fixed a bug that caused -1019 errors on random files on Windows clients (#2350)
- FIXED** Fixed a bug where creating and then removing a new network interface did not remove the interface (#2382)
- FIXED** Fixed a bug that caused repeat occurrences of Grooming error -2241 even after catalog rebuilds (#2414)
- FIXED** Log no longer shows "Manual Recycle" for a scheduled Media Set recycle operations (#2449)
- FIXED** Fixed a bug that caused assertion failure at "scsitools_mac.cpp-105" (#2455)
- IMPROVED** On-demand client features now default to enabled
- FIXED** Fixed a bug where scanning media slots in tape libraries also scanned import/export slots (#2554)
- FIXED** Fixed issue where "ignored" devices disappeared from UI after engine restart, making it impossible to re-enable the device (#2555)
- FIXED** Fixed a bug that caused Copy Media Set scripts to crash the engine with certain sources (#2569)
- FIXED** Fixed a UI issue where Retrospect did not show the correct value entered for number of backups to keep (#2832)
- IMPROVED** Made a change to support Mountain Lion's new sleep routines
- FIXED** Removed the unnecessary password field in Test Address window (#2938)
- FIXED** Copy scripts' "Copy System State" option now sticks properly (#2982)
- FIXED** Fixed Restore Windows security information setting not saving (#3007)
- FIXED** Fixed a bug that caused an assert while grooming: grx.cpp-1076 or grx.cpp-1078 (#3032)
- FIXED** Fixed a bug that could cause network Client updates to fail (#3078)

Known issues with this release

Files marked as private with the Retrospect Client are invisible to a Retrospect engine running on the same computer. This issue only occurs when the Retrospect engine and client software are both installed on the same Mac.

System Preference panes are not uninstalled from disks encrypted with FileVault whole disk encryption. To remove the Retrospect and Retrospect Client System Preference panes from disks encrypted with FileVault's whole disk encryption feature activated, right-click (or Control-click) on them in System Preferences and select the Remove option.

Media Sets with DES encryption created on PowerPC-based Macs running Retrospect 8 cannot be read by Intel-based Macs and vice versa. We recommend that users requiring data encryption switch to the more advanced AES standard.

Disk Media Set members cannot be edited on Mac OS X 10.5 64-bit Macs. We recommend running Mac OS X 10.6 “Snow Leopard” or later on 64-bit-capable Intel Macs.

Tape library magazine slot assignment changes do not update until the Retrospect console is quit and restarted.