Retrospect 8 for Windows
User's Guide Addendum

Introduction

This addendum to the Retrospect User's Guide describes new functionality introduced since the last revision of the Retrospect User's Guide. It is assumed that the user is already familiar with the operation of Retrospect in general, as well as the computing systems that Retrospect is used to protect. For a more thorough description of how to use Retrospect, please consult the Retrospect User's Guide.

In this guide

New Retrospect Client software

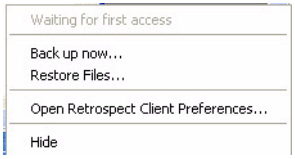
Retrospect Client software allows individual users to control aspects of the backup and restore operations performed on their computers. The client software has been redesigned for Windows and Mac OS. The changes include:

- 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* on page 8.

User-initiated backups and restores

Users now have the ability to restrict 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:

1. Click the Retrospect icon in the Windows taskbar or Mac OS menu bar.
2. Select **Back Up Now**.
3. Use the Backup Files and Folders dialog to select the items to back up.
4. 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.
- 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. See *History preferences* on page 6 for more information.

To perform a user-initiated restore:

1. Click the Retrospect icon on the client computer's taskbar or menu bar.
2. Select **Restore Files**.
3. In the Restore Files and Folders window, select a backup from the menu that contains the files you would like to restore.

   Retrospect will then retrieve a list of files contained in the selected backup. The list may take some time to load.
4. Select the files to restore.
5. Click **Restore**.

   If you are restoring files to a location that already exists, a confirmation dialog will appear.
6. To choose a different location, click **Browse**. To continue, click **Restore**.

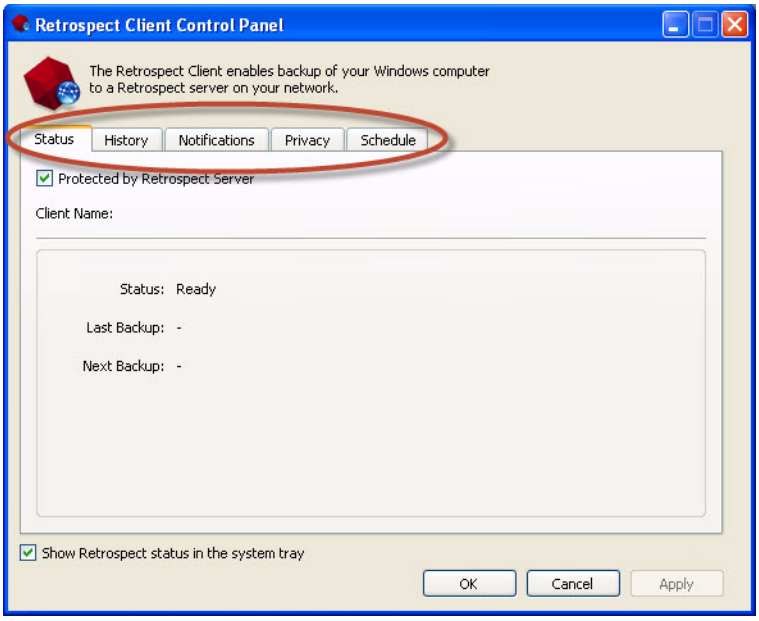
Improved client preferences

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 Proactive 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 proactive 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:

1. The lockout controls are in the Retrospect console. Choose **Configure** > **Preferences** > **Allow Clients to** in the Retrospect console sidebar.
2. 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 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.

To customize these default preferences for an individual client:

1. Select **Configure** > **Clients** in the Retrospect sidebar.
2. Select a client from the list.
3. Click **Properties**.
4. Modify the preference settings as desired for this client.
5. Repeat Step 1 to Step 4 for each client you wish to customize.

Disaster recovery

To successfully recover a computer that won't boot, it is first necessary to have a complete Retrospect backup of that computer's boot volume, as well as any other disks that you want to restore. In addition, you will need to have access to the Backup Set storage media containing the backup, as well as the Catalog file that matches the Backup Set. A comprehensive backup strategy should include making copies of Retrospect's Catalog files onto separate media, such as a network volume or another computer.

There are two methods for restoring a computer that won't boot:

- Boot the computer from a Retrospect Emergency Recovery Disc and perform a complete restore (fastest)
- Install a Windows operating system and the Retrospect application or Retrospect Client software, and then perform a complete restore as outlined in "Restoring from a Full Backup" on page 207 of the Retrospect User's Guide.

Creating a Retrospect Emergency Recovery Disc

The Disaster Recovery wizard will help you create an ISO image that can be burned onto a disc and used to boot your computer and restore it to a previous state in the event of a disaster, such as a hardware (e.g. hard drive) failure. In order to fully protect your system and the programs and data that reside on it, it is strongly recommended that you follow the steps below to create a bootable disc as soon as possible.

Before you create an ISO image, make sure you have the following items:

- The Microsoft Windows Automated Installation Kit (Windows AIK) installed on the computer where you will be running the Disaster Recovery wizard. Retrospect will give you the option to download the Windows AIK during the process.
- Any drivers or packages (i.e. package.cab) that you would like to add to the ISO image should be placed in the following directory **before** creating the ISO image.

  ```
  <retrospect application>/drsupp/drivers
  ```

- A blank optical disc

To create a bootable disc:

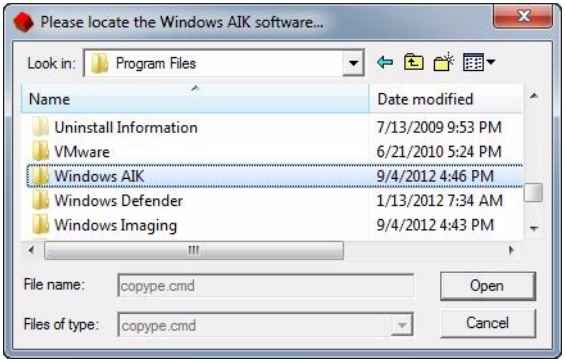
1. From the Retrospect navigation bar, go to **Backup** > **Disaster Recovery**.

2 Click **Next**.

You will then be asked for the Windows AIK software. Retrospect uses the AIK to create an Emergency Recovery Disc.

3 Click **Download the Microsoft Windows AIK image** link, or click **Browse...** if you have already downloaded and installed the software.

4 To locate the installed Windows AIK software, browse to the appropriate folder, then click **Open**.



You will then be asked to confirm the location of the Disaster Recovery CD-R image file.

5 Confirm the default location by clicking **Next**, or click **Browse...** to specify an alternate location.

The Disaster Recovery preparation should now be complete.

6 Burn the ISO image file onto an optical disc, and store it in a safe place.

Note: If you received any errors during the creation of the Disaster Recovery image (e.g. not enough disk space for the image), click **Open Log** to view the Retrospect Operations log file.

Using the Retrospect Emergency Recovery Disc

Once a Windows computer has been booted from the Retrospect Emergency Recovery Disc, its hard disk drives can be partitioned and formatted, and it can be restored either locally, by using the Retrospect application with connected storage media containing the backup, or from a Retrospect server on the network via the Retrospect Client software.

Note: The Retrospect Emergency Restore Disc and the Retrospect restore process are designed to restore to hardware similar to that from which the backup was made, such as when a hard disk drive is replaced, not when the destination computer is completely different from the source computer.

The Retrospect Dissimilar Hardware Restore add-on makes it possible to perform a complete restore to different hardware, such as when replacing a failed or lost computer with one from a different manufacturer. See "Making your system bootable on different hardware" on page 22 for more information.

Planning ahead

To successfully recover a computer that won't boot, it is first necessary to have a complete Retrospect backup of that computer's boot volume, as well as any other disks that you want to restore. In addition, you will need to have access to the Backup Set storage media containing the backup, as well as the Catalog file that matches the Backup Set. A comprehensive backup strategy should include making copies of Retrospect's Catalog files onto separate media, such as a network volume or another computer.

Note: If you do not have a copy of the Backup Set's Catalog file, it can be recreated from the media, though this will increase the length of time required to complete the restore.

Note: If you are restoring to a disk that had Windows Vista, 7, 8, Server 2008, or Server 2008 R2 or Server 2012 installed, the physical target hard disk drive must be the same size or larger than the physical drive being replaced. This is necessary to ensure the proper restoration of any hidden partitions, such as a Recovery Partition, that was present on the source disk.

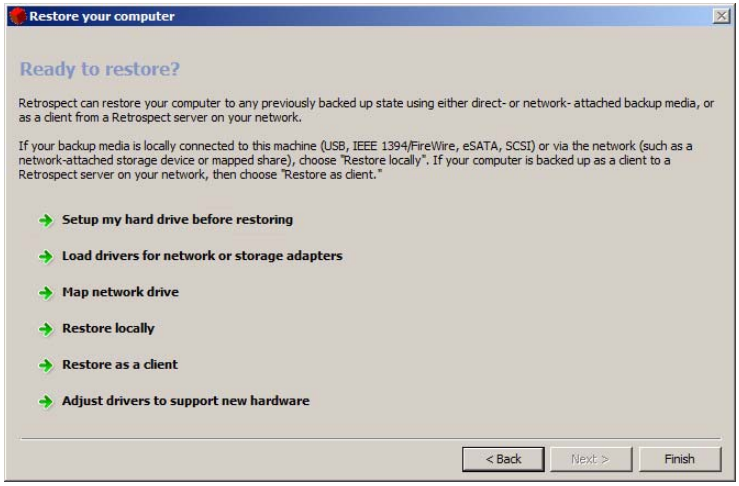
Getting started

If the computer you are recovering from a non-bootable state is the same computer that runs Retrospect, then you will be restoring locally, using the Retrospect application. If the computer you are recovering is normally backed up as a client to another computer on the network running the Retrospect application, then you will be restoring using the Retrospect Client method.

Insert the Retrospect Emergency Recovery Disc in the optical drive of the computer to be restored, power it on and boot from the disc.

Note: You may need to adjust the boot order in your computer's BIOS settings to boot from a disc. Refer to the documentation for your specific computer model for instructions on how to change the BIOS settings during the boot process.

Once you've booted from the Retrospect Emergency Recovery Disc and agreed to the legal notifications, you will be presented with the home screen of the Emergency Recovery wizard.



This screen provides access to all the tools needed to recover your computer. From here, you can partition and format your hard disk drive, install drivers for components required to access the network or storage devices, and map a network drive. Once the environment is configured with the aforementioned tools, you can choose to restore locally using the Retrospect application or as a client from a Retrospect server on the network.

Setting up your hard disk drive for recovery

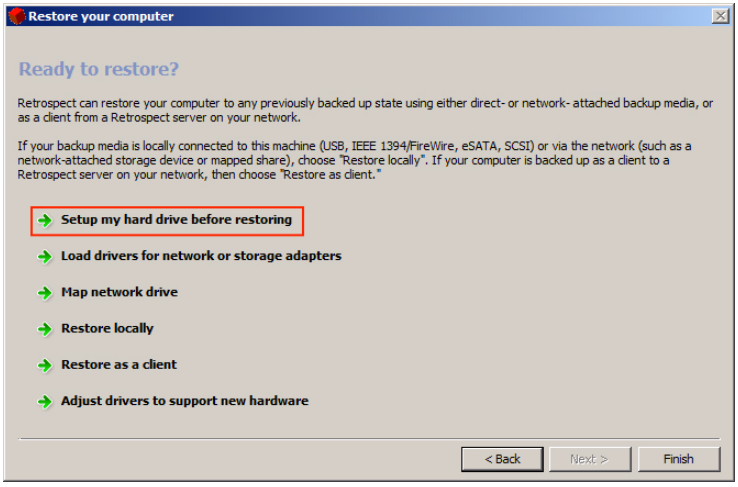
In some cases, you may need to partition or format the hard disk drive in your computer before you can proceed with the Emergency Recovery process. This is common practice, especially if you are replacing a smaller drive with a larger one.

Retrospect Disaster Recovery is intended for Windows-based computers and is restricted to OSes and file systems supported by Windows AIK. Refer to the following table for further examples of what is supported:

Action	Supported in this version?
Restoring RAID filesystems	No
Basic partitioning	Yes
Dynamic partitioning	No
Creating GUID partitions	No
Creating and deleting partitions	Yes
Resizing partitions	No

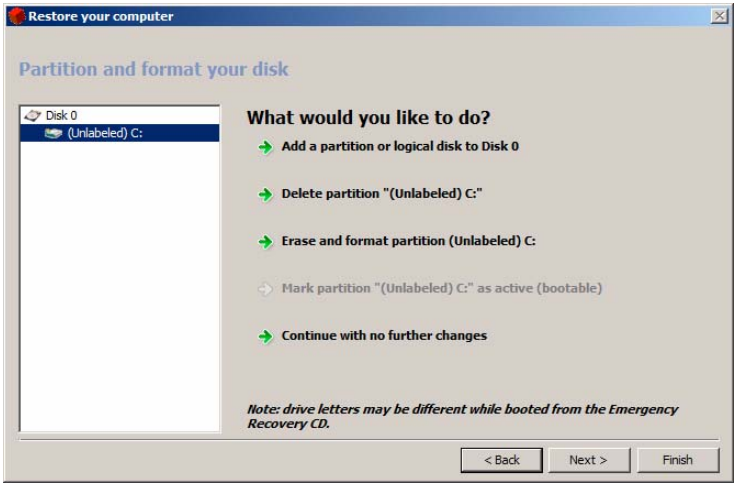
To partition and format a hard disk drive:

1 Click **Setup my hard drive before restoring** from the home screen of the Emergency Recovery wizard.



Note: A drive must have at least one active partition before recovery can take place.

The main hard drive setup screen appears.



2 Select a disk or partition from the list on the left hand side of the dialog, and make your selection from the options on the right.

The options to the right will change depending on which disk or partition you have selected on the left hand side of the dialog.

Warning: Partitioning or formatting a hard disk destroys data stored on the disk. Proceed only if you are certain that the data on the drive has been properly backed up.

Warning: If the drive that are restoring had a hidden Recovery Partition, the Retrospect Emergency Recovery process will recreate the exact partitioning scheme that was present when the backup being restored was originally created. This process will destroy all data present on the drive.

Loading drivers

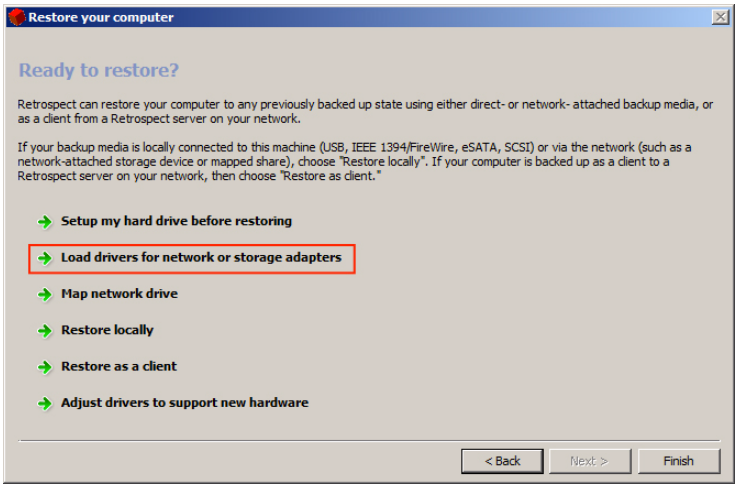
If the computer being recovered has a network adapter or storage host bus adapter that isn't recognized by the Retrospect Emergency Recovery system and that must be used in order to perform the recovery, it may be necessary to load a Windows driver for that adapter.

To install a driver:

1 Make sure that the driver is stored on media that is accessible by this computer.

Note: The driver should be located either on the network, an optical disk (the Retrospect Emergency Recovery Disc loads into RAM, so it can be safely ejected without affecting the recovery process), or even a USB flash drive.

2 Click on **Load drivers for network or storage adapters** from the home screen of the Emergency Recovery wizard.



A Windows file browser dialog appears.

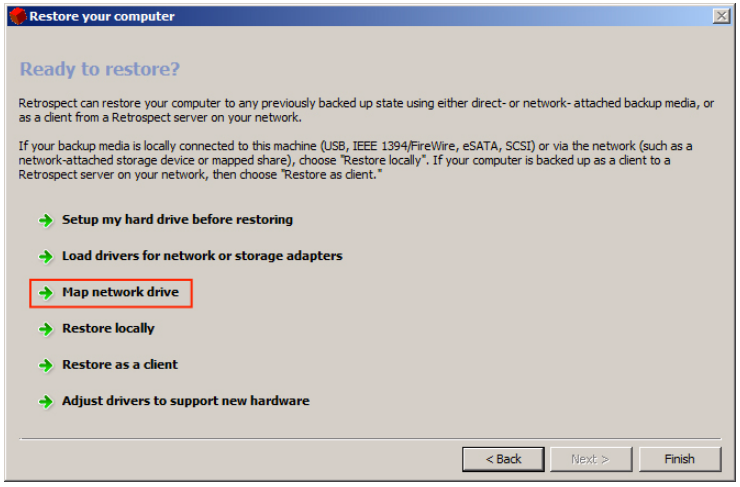
3 Browse to the location of the .inf file, then install.

Mapping a network drive

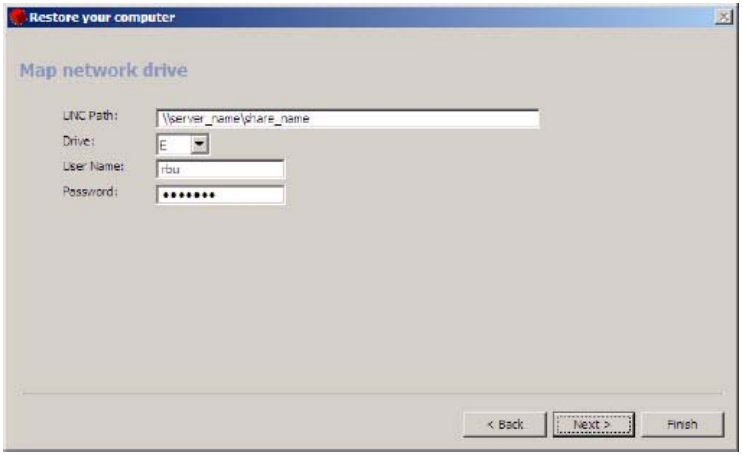
If you need to access a network share to complete the recovery process, a wizard will allow you to type a path and drive letter to map the volume to.

To map a network drive:

1 Click **Map network drive** from the home screen of the Emergency Recovery wizard.



The Map Network Drive Wizard appears.



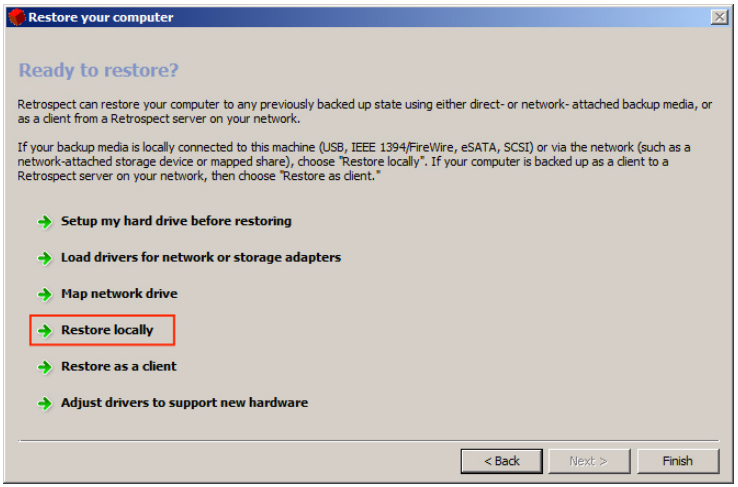
2 Type the UNC path to the share, assign a drive letter, and enter the proper login credentials in the spaces provided.

Restoring locally

If the computer being recovered was the Retrospect backup computer, you will be using the Retrospect application on this computer to restore from a Backup Set stored on either a locally-attached device, such as a USB hard disk drive or SCSI tape drive, or on a network volume.

To restore locally:

1 Click **Restore locally** from the home screen of the Emergency Recovery wizard, and use Retrospect to restore the computer as described in the Restore section of Chapter 4, "Immediate Operations," in the Retrospect User's Guide.



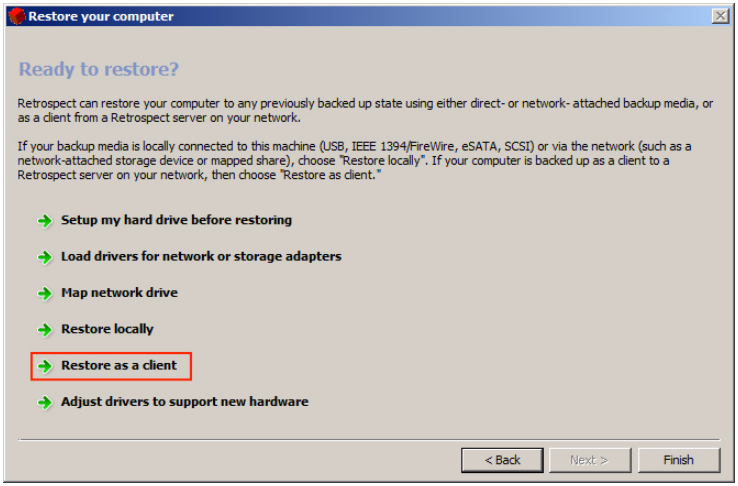
Note: When restoring the boot volume, make sure that you select a restore option that includes the registry and System State information, otherwise, the computer may not start up, and the Retrospect Emergency Recovery process will need to be repeated.

Restoring as a client

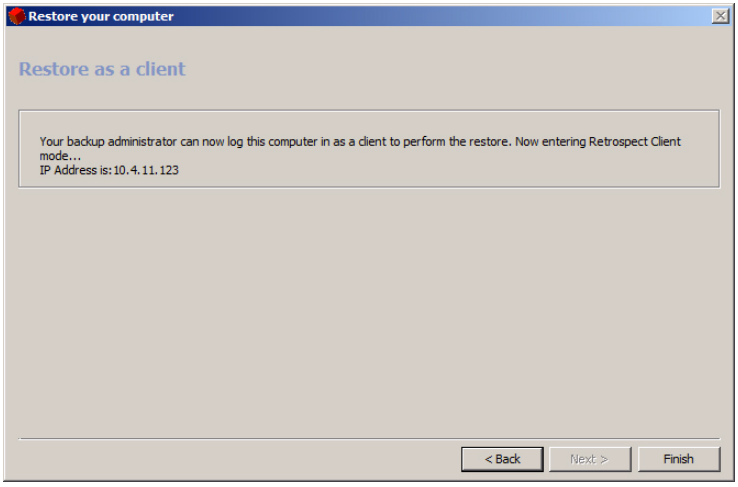
If the computer being recovered was being backed up as a client to a Retrospect server on the network, you will be restoring as a client.

To restore as a client:

1 Click **Restore as a client** from the home screen of the Emergency Recovery Wizard to initiate Retrospect Client mode.



A screen will appear, displaying the IP address to use in order to log this computer into the Retrospect server, as described in the Working with Clients section of Chapter 7, "Networked Clients," in the Retrospect User's Guide.



2 Once you have logged in this computer as a client to the Retrospect server, proceed to restore the computer as described in the Restore section of Chapter 4, "Immediate Operations," in the Retrospect User's Guide, selecting the client's volumes as the destinations for the restore.

Note: When restoring the boot volume, make sure that you select a restore option that includes the registry and System State information, otherwise, the computer may not start up, and the Retrospect Emergency Recovery process will need to be repeated.

Final steps

Note: If you created your Retrospect Recovery Disc from a Retrospect application that was licensed for the Dissimilar Hardware Restore add-on, you can now adjust the restored system to support the new hardware. **Do not** exit the disaster recovery wizard. Instead, follow the steps in the section "Making your system bootable on different hardware" on page 22.

When the restore is complete, exit Retrospect (if restoring locally), eject the Retrospect Emergency Recovery Disc, and click the **Finish** button in the Retrospect Emergency Recovery wizard to reboot the computer. In some cases a second reboot may be required.

If the computer being recovered was running Windows 7, 8, Windows Server 2008 or Server 2012, and a hidden Recovery Partition was present when it was previously backed up, then the Retrospect Emergency Recovery process will automatically re-partition the startup disk to match the original partition layout during the restore. This step is necessary for the computer to be able to start up properly following the restore.

If a hidden Recovery Partition was present and restored by Retrospect, you may need to adjust the hard disk partition sizes after the computer starts up normally. The most common need for this step is when a higher-capacity hard disk drive is used to replace full or failed lower-capacity hard drive. Because Retrospect must recreate the same partitioning scheme on the new drive, the extra capacity of the new drive will not be available for use until you extend an existing partition or create a new partition. Both of these tasks can be accomplished using Windows 7/8's or Windows Server 2008/2012's Disk Management tool.

Making your system bootable on different hardware

Following the disaster recovery restore, you can make your system bootable on different hardware by using the Retrospect Adjust OS Wizard.

Note: This option is only present if the Retrospect Emergency Recovery Disc was created with a version of Retrospect that was licensed for the Dissimilar Hardware Restore add-on.

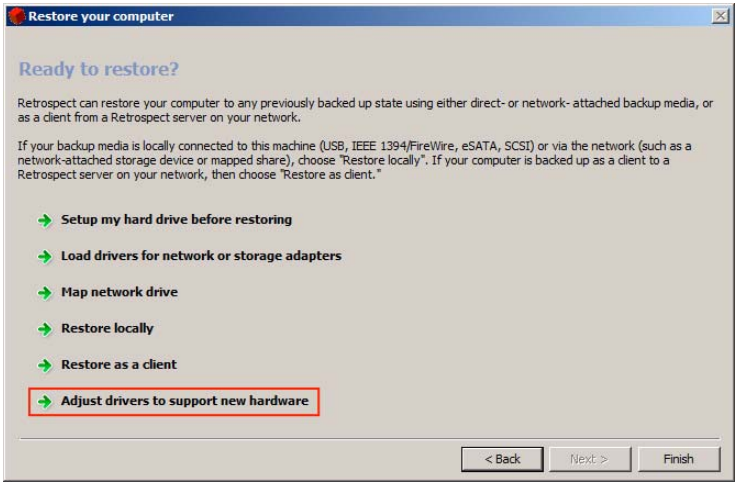
Before you start, make sure of the following:

- You have drivers for the new hardware that are ready to use, and are not zipped or located in .exe files.
- Your OS is located on the new computer, not in a backup image.

To make a Windows system bootable on different hardware:

Note: If you performed the complete restore locally using the Retrospect application, exit Retrospect now. If you performed the restore using the Retrospect Client, click the **Back** button. Or, if you already exited the Retrospect Disaster Recovery wizard, restart the computer; booting from the Retrospect Emergency Recovery Disc.

1 Click **Adjust drivers to support new hardware** to launch the Retrospect Adjust OS Wizard.

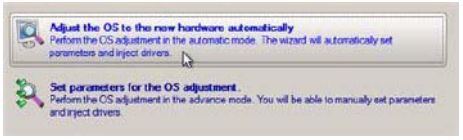


2 On the Wizard's Welcome page, click the **Next** button.

3 From the list of all found Windows systems (if there are more than one), select one that you need to adjust to the new hardware.

If you would like to adjust them all, re-launch this wizard for each Windows system.

4 Select **Adjust the OS to the new hardware automatically** if you do not plan to manually set any parameters for the OS adjustment.



If you are going to manually set parameters, see *Advanced scenario specifics* on page 26 for instructions on using the advanced mode.

When you select **Adjust the OS to the new hardware automatically**, the wizard will automatically begin executing the adjustment, and a progress bar will appear.

Note: In the event that the wizard fails to locate an additional driver repository, you may be asked to specify a path to the drivers required for some boot-critical drivers in the built-in Windows repository.

Hardware drivers for various operating systems are commonly located on removable media (CD or DVD) that arrived with the hardware packaging. Collect all of the drivers in one folder so the wizard can automatically pick and install those required for your OS.

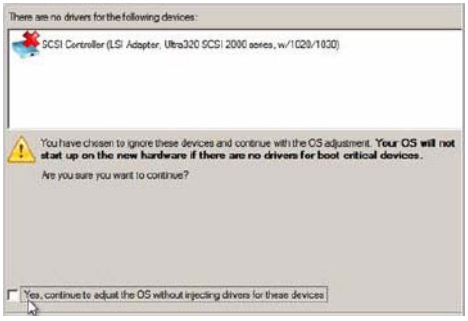
---

5 Select **Search for drivers in a specific folder**.

6 Click the link **What devices have no drivers?** at the bottom of the dialog to see if your boot-critical device does not require drivers.

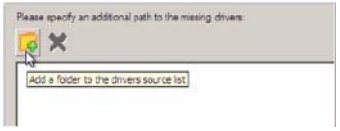
The wizard will name all devices according to their model description.

Caution: It is strongly recommended that you do **NOT** select the option **Yes, continue to adjust the OS without injecting drivers for these devices**. Choosing this option will likely result in Windows being unable to boot on the new hardware.



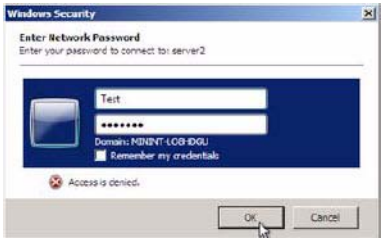
Retrospect Adjust OS Wizard will then need to locate the additional driver(s). In the event that the drivers are located on a network share, you will need to map the drive, as in the example below.

7 Click the **Add folder** button to specify an additional path to the missing drivers.

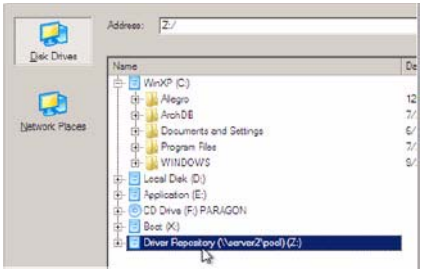


8 If the drivers are located on a network share, map the network drive by filling in the appropriate information.

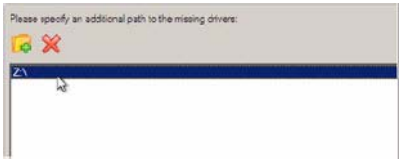
9 Enter your login credentials in the areas provided.



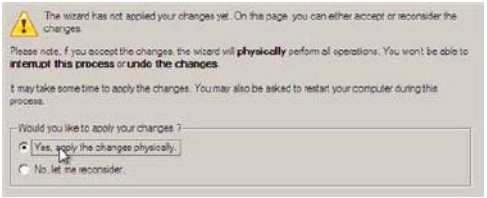
10 Select the location of the driver(s).



The wizard allows you to specify several driver repositories. When the wizard has located all of the missing drivers, you will then be asked to confirm the operation.



11 Select **Yes, apply the changes physically** to complete the operation.



When the operation is complete, the system will be bootable on the new hardware. After starting the system, Windows will initiate reconfiguration of all Plug and Play devices.

Advanced scenario specifics

You can use an advanced mode to manually set parameters for the OS adjustment, when prompted.

To manually set parameters for the OS adjustment:

1 Boot your computer from the Retrospect Emergency Recovery Disc.

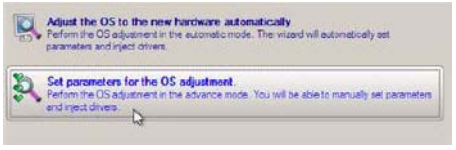
2 Launch the Retrospect Adjust OS Wizard.

3 On the Wizard's Welcome page, click the **Next** button.

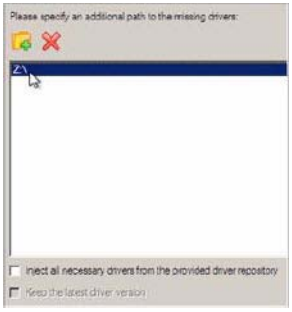
4 From the list of all found Windows systems (if there are more than one), select one that you need to adjust to the new hardware.

If you would like to adjust them all, re-launch this wizard for each Windows system.

5 Select **Set parameters for the OS adjustment**.



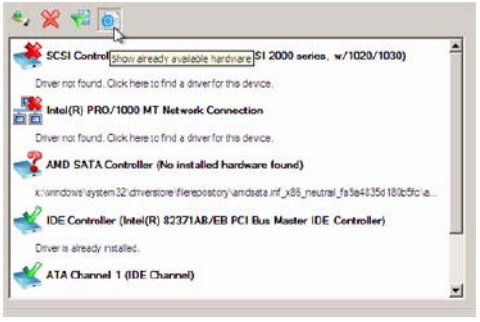
6 Specify an additional path to the missing drivers by browsing to the location.



You may also choose to select one of the following options at the bottom of the dialog:

- **Inject all necessary drivers from the provided driver repository** — Check this option to force injection of all drivers for your devices from the given driver repository, even if there are already installed drivers for some hardware. Use this option if you suspect that any of the installed drivers do not match your hardware.
- **Keep the latest driver version** — Check this option if you want to keep the latest version of the drivers during the forced re-injection. This option is only available when the **Inject all necessary drivers...** option, above, is selected.

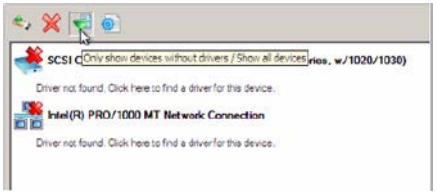
7 View all found hardware devices and their driver status by clicking the **Hardware Status** button.



The Adjust OS Wizard names all devices according to their model description.

8 Compare the listed devices with the given hardware to make sure the wizard has analyzed your system correctly.

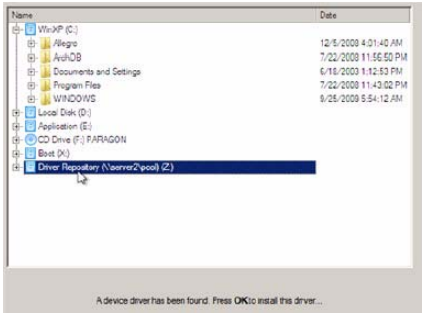
9 Filter your devices without drivers by clicking the **Filter** button.



You can use this option to view and inject drivers for network cards, as opposed to automatic mode where only boot-critical devices (i.e. storage controllers) without drivers are being reported.

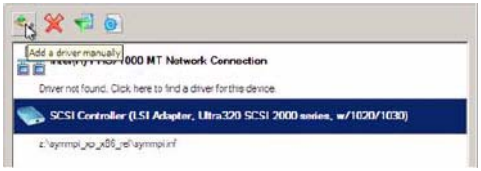
10 Add a driver for each device that is missing one by clicking on the device, then browsing for the required location.

The Retrospect Adjust OS Wizard will then match the device with the drivers in the given location, and select the right one.



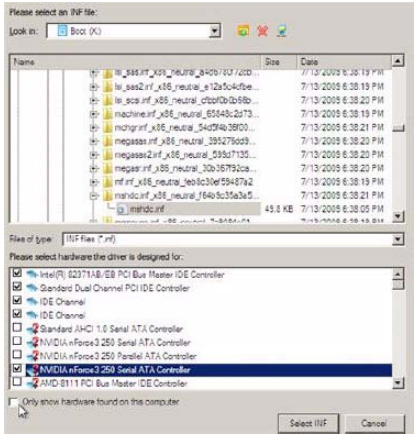
11 When the device driver has been found, click **OK** to install it.

12 You can manually add a driver for a device that has not been found by the Adjust OS Wizard by clicking the **Manual Driver** button.



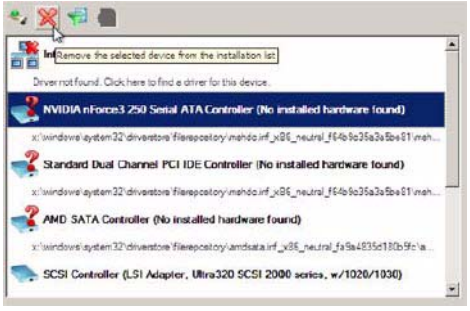
13 Specify the required .INF file by navigating to the appropriate location, selecting the .INF file, then selecting the corresponding hardware from the list.

14 Click the **Select INF** button.



Note: Use the **Only show hardware found on this computer** option to show/hide driver records for hardware.

15 You can remove a driver for a device which has not been found on your system by selecting it from the device list, then clicking the **Remove** button.



Protecting virtual machines with Retrospect and VMWare Consolidated Backup

Retrospect's integration with VMware Consolidated Backup (VCB) allows a Retrospect server running on a VCB proxy server to provide both file- and image-level backups and duplicates of a virtual machine (VM) without requiring the VM to be suspended or shut down. This is accomplished through Retrospect's External Scripting functionality, which calls the necessary pre- and post-scripts on the VCB proxy server.

Note: External Scripting is intended for advanced users who possess at least a rudimentary knowledge of one or more scripting languages supported by Windows Scripting Host. For more information, see the External Scripting section of Chapter 10, "Tools," in the Retrospect User's Guide.

Requirements

Before getting started with configuration, several prerequisites must be satisfied:

- A VCB proxy server must be setup, configured for its environment, and running as outlined in the Virtual Machine Backup Guide available from VMware's website at www.vmware.com.
- VMware Tools must be installed in each guest OS to be protected.
- Retrospect Disk-to-Disk or higher must be installed directly on the VCB proxy server. A Retrospect Multi Server license is required to back up or restore files directly to a guest server OS with the Retrospect Client running in a VM.
- The VCB proxy server must have enough disk space avail able to hold the largest image to be backed up or restored.
- This method of protecting VMs supports ESX 3 and 4; ESXi 5 is not supported by this method.

Configuring VCB for backups

Before configuring Retrospect to back up VMs, the VCB config.js settings file, located on the VCB proxy server (e.g. `C:\YOUR_VCB_FRAMEWORK\config\config.js`) must be modified. The variables that must be modified are:

```
BACKUPROOT=<path_to_mount>;                    (ex: BACKUPROOT="C:\\vcb_mnts";)
HOST=<esxserver_hostname>;                     (ex: HOST="esxserver.vmware.com";)
USERNAME=<user name>;                          (ex: USERNAME="vcbUser";)
PASSWORD=<password>;                           (ex: PASSWORD="vcbpasswd";)
VM_LOOKUP_METHOD="name";                       (ex: VM_LOOKUP_METHOD="name";)
PREEXISTING_MOUNTPOINT="delete";               (ex: PREEXISTING_MOUNTPOINT="delete";)
PREEXISTING_VCB_SNAPSHOT="delete";             (ex: PREEXISTING_VCB_SNAPSHOT="delete";)
```

Configuring Retrospect and Backing Up

Most of the work necessary prior to running backups of VMs takes place in the Retrospect Event Handler script and the Retrospect application.

Editing the retro.ini File

In order for Retrospect to communicate with VCB, the retro.ini file located in the Retrospect application directory must be edited. Open the retro.ini file with a text editor and add the following line in the [OEM] section:

```
CheckVCBScripts=1
```

- Save and close the retro.ini file.

The default install location for the Retrospect application is:

```
C:\Program Files\Retrospect\Retrospect 8.0
```

Retrospect Event Handler Settings

The Retrospect Event Handler is an external script through which Retrospect communicates information to other programs. VCB scripting is handled with a special Retrospect Event Handler, VCB_RetroEventHandler.bat. A sample script is provided in the External Scripts folder located in the application directory.

The default install location is:

```
C:\Program Files\Retrospect\Retrospect 8.0\External Scripts\Sample VCB
```

Note: It is recommended that a copy of the VCB_RetroEventHandler.bat file be created before any changes are made.

Configuring the VCB_RetroEventHandler.bat file is straightforward; only the `VCB_FRAMEWORK_PATH` variable needs to be set:

```
set VCB_FRAMEWORK_PATH=c:\vcb_framework
```

Activating the VCB_RetroEventHandler

To activate the `VCB_RetroHandler.bat` script, copy it to the same folder as the Retrospect Config file.

For Windows XP and Server 2003:

```
c:\Documents and Settings\All Users\Application Data\Retrospect\;
```

For Windows Vista and Windows 7:

```
c:\Users\All Users\Retrospect\
```

For Windows 8, Server 2008 and Server 2012:

```
c:\Application Data\Retrospect\
```

Creating Virtual Machine Backup Scripts

The following process needs to be repeated for each VM and each type of backup (file or image).

To create Virtual Machine Backup Scripts:

1. Create a temporary folder in the VCB mount points directory which is specified by the variable BACKUPROOT in VCB config.js (see "Configuring VCB for backups" on page 30).

   To perform an **image-level** backup of a VM named mytestvm.foo.com, the folder must be named:

   ```
   C:\vcb_mnts\mytestvm.foo.com-fullVM
   ```

   To perform a file-level backup, the folder must be named:

   ```
   C:\vcb_mnts\mytestvm.foo.com
   ```

2. Define the mount point as a subvolume in Retrospect.
3. Define a backup script with a name beginning with `VCB_` (e.g. `VCB_mytestvm_backup`) and specify the subvolume defined above as source.

   Once all of the above steps have been completed, Retrospect is ready to back up VMs.

Note: For file-level backups, when VCB mounts a VM's drive, folder and file hierarchy, it creates identical views within two directories, one called "letters" and other called "digits". Retrospect only backs up the contents from directory letters.

Restoring Data to Virtual Machines

For each type of backup, either file-based or image-based, there is a corresponding restore method. Data from file-level backups are typically restored via Retrospect Client software running in the VM, whereas image-based backups are first restored to a directory on the VCB proxy server before being moved to the ESX or vCenter Server using VMware Converter.

Restoring from File-Level Backups

File-level backups provide the ability to restore individual files to any

physical or virtual computer that is running the Retrospect Client software. Because Retrospect backs up the file and folder structure from a VCB mount points directory, which buries the virtual volumes inside additional levels of folder hierarchy, this method does not allow for full machine restores.

To perform folder and file-level restores using the Retrospect Client software installed inside a VM, refer to Chapter 4 of the Retrospect User's Guide.

Restoring from Image-Level Backups

While image-level backups of VMs don't allow for smaller, incremental backups, they do provide the very fastest complete restore of an entire VM. Restoring from an image-level backup is a two-step process. First, use Retrospect to restore the VM image (usually made up of multiple .vmdk files) to a new folder on the VCB proxy server. Once that step is completed, use one of the methods outlined in VMware's Virtual Machine Backup Guide to complete the process of restoring the image to ESX or vCenter Server storage.

Other improvements

Retrospect8 includes these additional new features:

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 Backup Set.

Support for Win 8 and Win Server 2012

Both the Retrospect application and the Retrospect Client software support Windows 8 and Windows Server 2012.

Support for Mac OS 10.8 “Mountain Lion”

The Retrospect application now supports the Retrospect Client software running on Mac OS X 10.8 Mountain Lion and Mac OS X 10.8 Mountain Lion Server.

Backing up to the Cloud

Retrospect 8 supports backing up to Internet-connected (cloud) storage using the WebDAV protocol. Before a WebDAV volume can be used in a disk Backup set or as a source for backups, it must first be set up by going to **Configure** > **Volumes**, as described in the Retrospect User’s Guide (see “To add a network volume to the volumes database” on page 282). Use `http` or `https` when entering the UNC path.