



# Highly Reliable Systems



## High-Rely Backup System Documentation





# READ THIS FIRST

## Important Quick Start Information for your High-Rely drive

- **DO NOT ATTEMPT TO REMOVE High-Rely media from their drive bays without “unlocking” the drive with the key first! Forced removal of the drive will void your warranty. The key has a mechanical interlock that blocks the drive from being removed.** Each pre-installed HR drive is shipped in the locked and “on” position. Refer to page 12 through 15 of your manual if you have difficulty.
- **High-Rely media will not “power up” until the key lock on the front of the drive is turned to the locked and on position. This is by design and prevents accidental media removal. Refer to page 12 through 15 of your manual.**
- The latest Service Packs are important! Microsoft has continued to Debug USB-2.0 on the Windows 2000, XP, and 2003 product lines. If you do not have Service Pack 4 on Windows 2000 or Service pack 1 on XP you may have problems. For example, XP machines without SP1 cannot properly recognize drives above 137GB. While it may appear to work the drive will corrupt data when it fills above that level. Read the manual or our web site for more details.
- Not all USB 2.0 ports are created equally. We recommend those based on the NEC chip set for maximum compatibility. Problems with low quality ports can range from slow performance to intermittent “Delayed Write Cache” failures in Windows.
- **Before HR media is removed from any High-Rely drive the Windows operating system should be notified. To do so choose “Safely remove Hardware” from the Tool tray.** Please see the section of this manual titled “safely removing the media”.
- If you use Veritas Backup Exec, only version 9.0 or higher should be used. Always choose the “Backup to Removable Disk” folder. Never use the “Backup to Disk folder” since Backup Exec may become confused when restoring data from removable drives.
- The information in this manual primarily documents Windows 2000, 2003, XP and Vista systems. Although the High-Rely will work with Windows 98 and the supplied drivers, the High-Rely Disk Management software, which affects ease of use, does not support Windows 98.



<a href="#">Introduction.....</a>	<a href="#">6</a>
<a href="#">Benefits of the High-Rely System.....</a>	<a href="#">8</a>
<a href="#">Compatibility.....</a>	<a href="#">8</a>
<a href="#">Convenience.....</a>	<a href="#">8</a>
<a href="#">Speed.....</a>	<a href="#">8</a>
<a href="#">Reliability.....</a>	<a href="#">9</a>
<a href="#">Media.....</a>	<a href="#">9</a>
<a href="#">Portability.....</a>	<a href="#">9</a>
<a href="#">Cost.....</a>	<a href="#">9</a>
<a href="#">Warranty.....</a>	<a href="#">10</a>
<a href="#">A Word of Caution.....</a>	<a href="#">10</a>
<a href="#">Connecting a High-Rely Unit to Your Computer.....</a>	<a href="#">11</a>
<a href="#">Internal Units.....</a>	<a href="#">11</a>
<a href="#">PCI USB 2.0 Port.....</a>	<a href="#">11</a>
<a href="#">Motherboard USB 2.0 port.....</a>	<a href="#">11</a>
<a href="#">External Units.....</a>	<a href="#">14</a>
<a href="#">Inserting the Media.....</a>	<a href="#">15</a>
<a href="#">Using the High-Rely Display and Interface.....</a>	<a href="#">18</a>
<a href="#">Understanding the LCD Display.....</a>	<a href="#">18</a>
<a href="#">Programming the Temperature Alarms.....</a>	<a href="#">19</a>
<a href="#">Silencing an Alarm.....</a>	<a href="#">19</a>
<a href="#">Using Devcon to Safely Remove Drives.....</a>	<a href="#">22</a>
<a href="#">A Note About the “Optimize for Quick Removal” Option.....</a>	<a href="#">23</a>
<a href="#">Assigning Drive Letters on Windows Systems.....</a>	<a href="#">24</a>
<a href="#">Assigning Drive Letters with Microsoft’s Disk Management Program.....</a>	<a href="#">25</a>
<a href="#">Disk Management Tips and Tricks.....</a>	<a href="#">27</a>
.....	<a href="#">27</a>
<a href="#">Understanding the High-Rely Drive Manager.....</a>	<a href="#">28</a>
<a href="#">Installation of the High-Rely Drive Manager.....</a>	<a href="#">28</a>
<a href="#">Follow the on-screen instructions for installation of the High-Rely Drive Manager and consult the on-line help in the HRDM2 administrator when needed.....</a>	<a href="#">29</a>
<a href="#">The Backup Process – An Overview.....</a>	<a href="#">29</a>
<a href="#">How Hard Drives Work and Why They Fail.....</a>	<a href="#">30</a>
<a href="#">Top 10 Common Backup Mistakes.....</a>	<a href="#">33</a>
<a href="#">Backup Software.....</a>	<a href="#">34</a>
<a href="#">Using Windows NTBackup.....</a>	<a href="#">35</a>
<a href="#">A Note about NTBackup under XP Home Edition.....</a>	<a href="#">35</a>
<a href="#">Backup Rotation Schemes.....</a>	<a href="#">38</a>
<a href="#">XP Professional and Windows 2003 - Volume shadow copy.....</a>	<a href="#">38</a>
<a href="#">Scheduling the Job.....</a>	<a href="#">38</a>
<a href="#">Backing up System State with NTBackup Two Stage Backups.....</a>	<a href="#">40</a>
<a href="#">NTBackup Review Checklist.....</a>	<a href="#">40</a>
1. <a href="#">Reviewing Backup File Time and Date.....</a>	<a href="#">41</a>
2. <a href="#">Reviewing Your NTBackup Size.....</a>	<a href="#">41</a>
3. <a href="#">Reviewing the NTBackup Logs (Reports).....</a>	<a href="#">43</a>
4. <a href="#">Reviewing NTBackup Performance.....</a>	<a href="#">46</a>



<a href="#">5. Checking The Event Viewer for NTBackup problems.....</a>	<a href="#">47</a>
<a href="#">Application Log.....</a>	<a href="#">49</a>
<a href="#">System Log.....</a>	<a href="#">49</a>
<a href="#">Monitoring NTbackup.....</a>	<a href="#">51</a>
<a href="#">Backing Up Microsoft Exchange with NTbackup.....</a>	<a href="#">51</a>
<a href="#">An Alternative Exchange Mailbox backup Method.....</a>	<a href="#">52</a>



## Introduction

Through the years, hard drives have become more reliable. However, hard drives can still wear out or break down for a variety of reasons. When this happens, it leaves you vulnerable to losing valuable business data. Perhaps even more important when considering reasons to backup are inadvertent data corruption and viruses. Traditionally some sort of tape has been used to backup computers due to its low cost and portability. Unfortunately, tape has proven to be extremely problematic, slow, and - in many cases - untrustworthy.

At Highly Reliable Systems we believe a good backup device should have some or all of the following features to accommodate a solid backup strategy:

- The Backup Media can be easily transported off site.
- The Backup Media should be extremely cheap per Gigabyte of storage
- The entire network backup should ideally fit onto one removable media so it can be done at night unattended.
- The Backup process should be fast.
- Multiple media should be used so that a history of data can be maintained over a period of time.
- The backup drive itself should be reasonably priced.
- The data should be available to restore immediately using “random access” to any file
- The backup should have a long “shelf life”.
- Backup media should be transportable and usable in a wide variety of systems.
- The Backup media should be readily available.

Unfortunately, in today’s market, tape devices don’t give us all of the features on the list above. While inexpensive tape drives do exist, more reliable tape drives are expensive. We argue that “truly” reliable tape drives don’t exist at a reasonable price. This opinion is based upon many years of frustration in the field trying to make them work. Tapes are a “streaming” media, and unlike hard drives, which are “random access” require fast forwarding or rewinding to get to individual files. This process is time consuming and fraught with errors.

Have you ever been driving along and noticed black streamers of tape from a mutilated music cassette trapped in the weeds and billowing in the wind at the side of the road? Do you think the frustrated motorist who threw that tape out the window did so because it worked? Not likely. If you are frustrated with tape, we hope you will enjoy the High-Rely system. We believe that tape is antiquated, unreliable, and slow. We think you will be extremely pleased at the flexibility your new High-Rely media gives you when compared to tape. Although the cost per Gigabyte of storage for tape continues to be



relatively low, we believe that the failure rate is such that even with slightly higher media costs the high-rely solution is much cheaper overall.



## Benefits of the High-Rely System



By converting standard hard drives to USB 2.0 and using our unique removable drive trays, this backup drive makes all forms of tape backup obsolete! This system is faster, less expensive, and far more reliable than tape backup. It works with Windows 98, Windows 2000, Windows XP, and Windows 2003 and Vista systems.

### Compatibility

Due to the complexity of tape drives and the need for detailed logs to track backup results, most firms pay big dollars for third party tape backup software. Our multi-drive products show up as simple drive letters on your system and are trivial to use, so using the standard backup software and scheduler that come with your operating system becomes much more practical. Or, if you prefer, you can still use third party software that supports removable drives such as Veritas Backup Exec 9.0, or Computer Associate's Brightstor Arcserve. You can even use it with popular drive imaging software such as Acronis True Image, Symantec Ghost, or Drive Image! Available in both external, multi-bay and internal versions, there has never been a better time to buy your last tape.

### Convenience

Imagine not having to swap tapes out daily. Our multi-drive backup solutions allow you to direct different backup jobs to separate removable drives each day of the week. Then simply swap all the drives out one time at the end of the week and take whatever is needed off site for added disaster recovery protection. Get the functionality of a robotic "tape library" at a fraction of the cost and with more reliable and stable media!

### Speed

We've benchmarked the backup speed over USB 2.0 and compared it to typical SCSI tape drives. USB 2.0 allows the High-Rely drive to beat tape in almost every scenario. No rewinding or "drive hitching" back and forth - just fast, reliable smooth backup and restore. Using MP3 files and the bundled NTI Backup Now software without compression, we have seen "real world" transfer speeds of 70Gigabytes



per hour to a high-rely drive. Even faster results are possible using low level “sector based” copy software. Although we cannot guarantee a particular speed with your system and files due to the variables involved, we firmly believe you will see much faster backup results than if you used any type of tape.

## **Reliability**

Tape vendors are fond of quoting hundreds of thousands of operations before their tapes wear out. In the real world most of our customers report tapes last at most a year before unaccountable and frustrating errors start to occur. Using our technology, we guarantee your HR media will last for a minimum of 18 months. For a nominal warranty upgrade fee, we will provide a limited warranty for your drive and media for a full 3 years. Since our HR backup media is based on IDE hard drives, the stability and reliability is well established. Each HR drive tray has its own independent fan and temperature alarm to insure reliable operation. Any temperature problems result in immediate audible alarm.

## **Media**

Our drives support all standard drive sizes including the newer 750+ Gigabyte drives. You can buy the removable HR tray with our pre-formatted and tested IDE drives already installed. These drives have our unique 18 month replacement warranty. Or.... buy the trays separately and use your own drives. Tape vendors argue that tapes cost far less than hard drives. However, real world experience shows us tapes wear out about 10 times faster! Hard drive media cost slightly more initially but you will save money in the long run because the drives will last longer, have more repetitive uses, and save you many, many hours of waiting for rewinds, back-hitching, and frustrating failed restores.

Tape vendors frequently quote tape capacity with two numbers such as 12/24 or 40/80. This second number represents the size of compressed data that will fit on a tape. So a 40/80 tape is actually natively 40GB in capacity. The manufacturer “hopes” your data will compress 2 to 1! If you are using the NTFS file system or a third party backup software the same compression used for tapes can be used for HR media. Thus, our 5 drive 120GB HR drive, when used with compression, could store an impressive 1.2 Terabytes of backup data!

## **Portability**

Traditional tape solutions can have portability problems due to head alignment and software issues making it difficult to move tape data from one machine to another. Our drives are formatted to the operating system and can not only be moved from one machine to another by simply plugging into any USB 2.0 or 1.1 port, they can be moved without ever powering down either machine. In addition, IDE drives can be removed from their portable USB trays and installed on traditional IDE controller cables and used without reformatting or loss of data.

## **Cost**

You would expect all this would come at a higher price tag than tape. However, a 5 drive HR solution is priced comparably to a single high end tape drive that use technologies such as DAT, DLT, and AIT. Chances are you already have a USB 2.0 controller in your machine. If not, one can be added at a price far below the traditional SCSI controller required for tape drives.



## **Warranty**

Our company name says it all. We design our systems for hard daily use. The High-Rely drives and media come with either 1 year or 18 month limited warranty (depending on your unit and whether it was purchased as a bundle or individually) that will repair or replace any component within 7 working days (typical). Your time is valuable! Since HR drives “just work” you won’t spend hours on the phone to our technical support reloading software, drivers, and running cleaning tapes. For added coverage please purchase our extended 3 year warranty which includes overnight replacement protection.

## **A Word of Caution**

No backup system is perfect and we know of none that can be completely ignored. It is very important that you check your backup logs on a regular basis, and insure that your backups are restorable. While we firmly believe you will find the High-Rely systems much more reliable than tape, we in no way can be responsible for lost or missing data or business losses associated with them. Please follow best practice recommendations by backing up often, insuring all critical files are included in the backup, transporting media off-site, and doing full test restores periodically.



## Connecting a High-Rely Unit to Your Computer

### ***Internal Units***

If you are installing an internal unit, you will be cabling the drive either directly to your motherboard or to an internally installed PCI card. The cables you will use for these two situations are different. Both types of cables ship with the internal units. Refer to the relevant section below for your situation.

### **PCI USB 2.0 Port**

If you are installing an internal PCI card, the card should have female USB-A style (flat) connectors “internal” to the PC chassis. The cable you will use has a “Pan-Pacific” (flat white wafer) connector on one side and a Male USB-A connector on the other. Many PCI cards have multiple connectors and any of the ports should be acceptable. The connectors are designed to go on only one way. Simply attach the cable to the back of the internal High-Rely drive and the PCI card, making sure to thread the cable to avoid fans and other moving parts.

### **Motherboard USB 2.0 port**

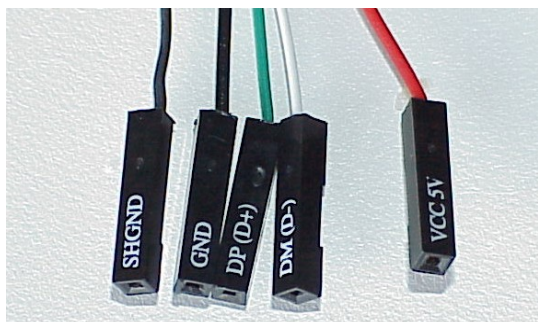
The Internal High-Rely drives ship with a “Pan-Pacific” (flat white wafer) connector on one side and 5 individual header pin connectors on the other. This cable is used to connect your internally mounted drive to the USB 2.0 ports on your motherboard. Most configurations will use this cable because most newer motherboards support USB 2.0. If you have doubts about compatibility, please consider installing an NEC chip based PCI card. Please be careful about static electricity when installing the cable. Static on your body can transfer to the motherboard (even when you don’t feel or see a static shock) and damage it. Always touch ground or use a grounded wrist strap before installing the cable. The Pan Pacific connector should connect to the back of your High-Rely drive and will only go on one way. The “loose” connectors must be put on according to your motherboard documentation.

The reason for the seemingly odd connector configuration on the motherboard side is that different motherboards have different header layouts for their USB 2.0 connectors. By creating separate





connectors we have allowed you to accommodate any motherboard layout.



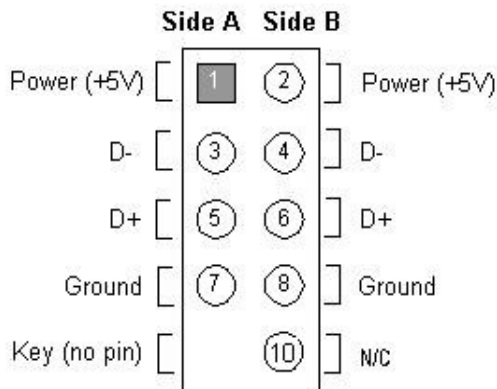
You will notice your High-Rely cable has color coded wires, as well as clearly labeled signal names on the black header connectors.

We have found that most motherboards use the “Intel” standard two row header as shown below. Such a connector usually provides TWO separate USB-2.0 connections. Your High-Rely can be connected to either side but should be plugged in a straight row (to either pins 1,3,5,7 OR 2,4,6,8)

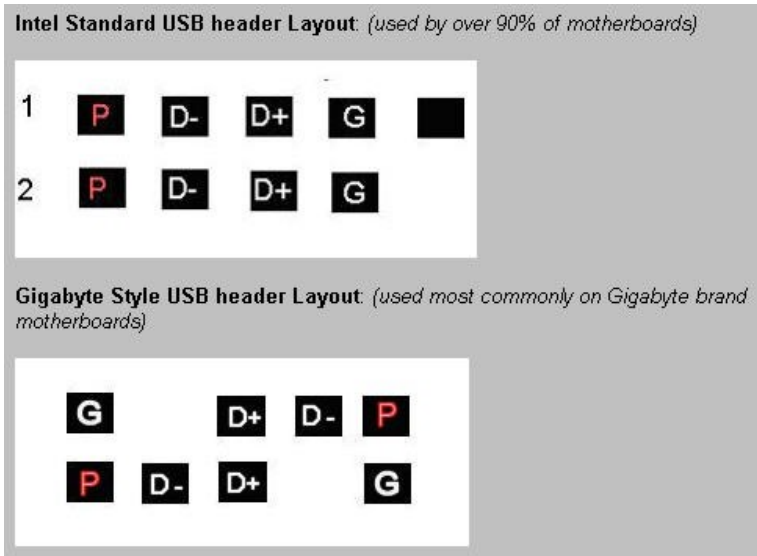


- ← Red Wire (5 Volt Power) Pin 1 or 2
- ← White Wire (Data - ) Pin 3 or 4
- ← Green Wire (Data + ) Pin 5 or 6
- ← Black Wire (Signal GND) Pin 7 or 8
- ← Black Wire (Shield GND) No connect

**Table: Front Panel USB Connector**



**Please consult your motherboard manual to confirm whether this layout matches yours.** We cannot be responsible for damage caused by hooking cables up incorrectly. The graphic below shows yet another representation of the Intel standard USB header (This is the same layout as depicted above but shown horizontally) along with an alternate layout used by some Gigabyte brand motherboards.



From the above

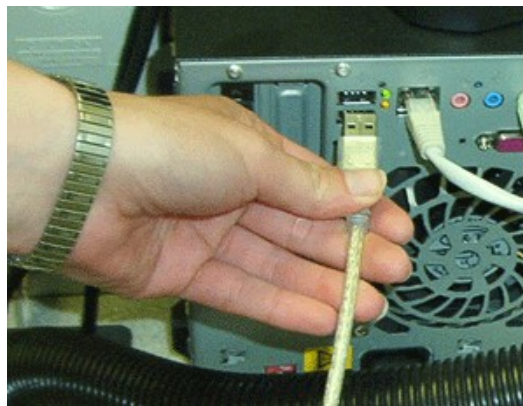
You should always power down your system when connecting the internal USB cables and double check your work by confirming the color codes to the signals depicted in your motherboard manual.

If you do not have USB 2.0 ports on your motherboard you will need to order a USB 2.0 card with an internal connector. We would recommend one based on the NEC chip set. The cable needed in this case will be different and is also included.

After connecting the data cable, simply connect any available standard molex power supply connector to the back of your High-Rely internal drive to provide DC power. Then mount the unit in your case as you would a standard CD or other 5.25" device. Some cases may require special "rails" or other mounting hardware that you will have to get from the case vendor.

## **External Units**

Regardless of what external model you have, the procedure to connect the external drive to your computer is the same. USB-2.0 has the ability to be plugged in "hot" (while your computer is already powered up) so if your computer already has the latest service packs and a compatible USB 2.0 port you may be able to install the High-Rely external drive without even powering down your system! Simply plug the USB-"B" connector side of the cable into the back of the High-Rely unit and the flat "A" connector to the USB-2.0 port on your computer as shown below.



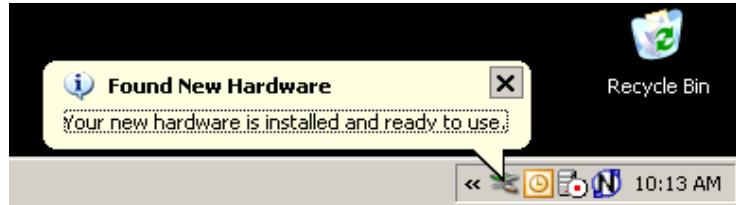
Now plug the High-Rely system into a power outlet that is protected by either a surge protector or a battery backup System (UPS) and power the unit on by pushing and holding the power button in for a moment.

Depending on the version and service pack level of your operating system, Windows (versions 2000, 2003, XP) should automatically detect the High-Rely system. On Windows 98 machines you will need to install the driver software supplied on the CD. Windows 95, NT and below are not supported. Linux and other operating systems that support USB 2.0 should also see the drive come



on line automatically. If your service packs are not up to date, it is possible that your system will install only a USB 1.1 driver, resulting in very slow backup times.

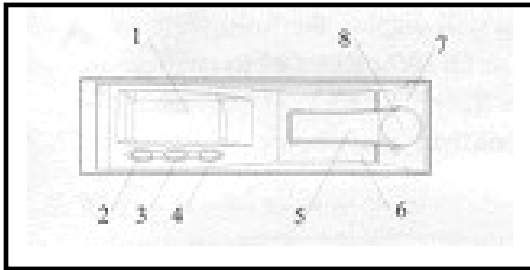
If your machine was already booted when you plugged the HR system in, you should wait until you see the following message in your system tray:



At this point, the system is online, and you can insert your HR media if you have not already done so.

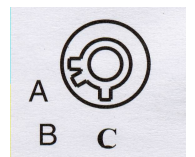
## Inserting the Media

The following diagram identifies the front of the HR removable drive and gives the names of each item. To remove the media properly you will need to understand the function of the release levers and the key lock mechanism (items 5, 6, and 8).

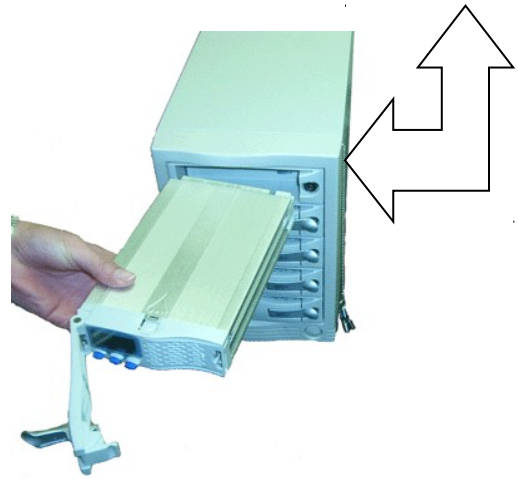


1. LCD Display
2. Set Button
3. Up button
4. Down button
5. Lock cover lever (Small lever)
6. Release Lever (Large lever)
7. Front Bezel of HR Receiver Frame
8. Hidden Key Lock

The High-Rely backup system makes use of IDE hard drives that use special electronics to convert them to use a USB 2.0 port. This allows the drives to be removed and installed while computer power is on (Hot swapped).

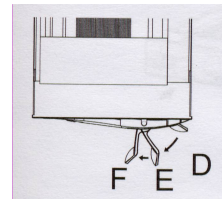


To insert the media, first make sure the lock is in the unlocked position (position C). Proper orientation of the removable drive is with the blue buttons to the left as shown in the photo. Notice that the entire large lever, called the “release lever” is in the fully open position. Do not attempt to insert the drive with the release lever closed.



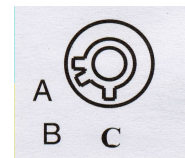
Push the drive all the way in until you feel resistance. At this time move the small lever (the “lock cover” lever) to its midway (position E).

Move the larger “release lever” towards the closed position, using the lever action of the mechanism to pull the drive in the last few centimeters. Close the release lever until it snaps. If it will not snap shut check to ensure that you have the smaller lock cover lever in the partially closed position E.



Lock Cover lever position E is used to insure the larger “release lever” will snap shut

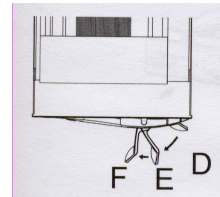
Now insert the key and turn it clockwise to the “A” position to power up the drive as shown in the photo. The B position of the lock is considered “off” and is not used in the High-Rely system.



At this point, if master power to the unit is on, you should see the LCD front panel of the drive light up and possibly hear the hard drive spin up. If you do not, the drive is not seated properly. Remove it and try re-seating it. Once you have successfully powered up the drive you should flip the lock cover to the fully closed or D position.



Once the drives spin up, Windows should recognize the new drive and will dynamically assign a drive letter to your new media. Please read the “Assigning Drive Letters on Windows” section for more information about changing the assigned drive letters.

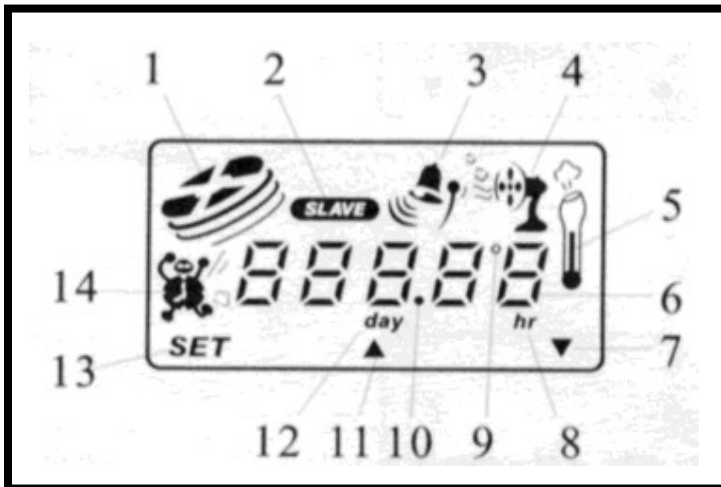


In the final step the “Lock Cover” should be moved to position D



# Using the High-Rely Display and Interface

## Understanding the LCD Display



1. Hard Drive activity symbol (simulates spinning disk when drive is in use)
2. Master/Slave Status display (Unused feature of the LCD display. Always displays as slave)
3. Alert Symbol (Symbol is on when the unit is in alarm status)
4. Fan Status Display (Simulates a rotating fan to show that drive fan is spinning)
5. Thermometer Symbol (On when numeric display is showing temperature)
6. Digit display (Displays temperature normally)
7. Down arrow (positioned above down button)
8. Hour Indicator (On when numeric display is showing days/hours of operation)
9. Degrees Symbol (On when numeric display is showing temperature)
10. Decimal Point
11. Up arrow (positioned above up button)
12. Day Indicator (On when numeric display is showing days/hours of operation)
13. SET indicator (positioned above SET button)
14. Hard Drive Usage Time Symbol (On when display is showing days/hours of operation)

### Normal Display

The normal LCD display will show the current drive temperature digits (6) in either Celsius or Fahrenheit. In addition, you should see the “slave” symbol (2), which is always on, the fan symbol simulating a spinning fan(4), the thermometer symbol (5), as well as the up and down arrow and SET symbols (7,11,13).

### Hard Drive in Use

When the hard drive is being written to or read from the hard drive symbol (1) will simulate a spinning disk. The rest of the display will be normal as discussed directly above.



### **Hard Drive Usage Display**

When you change the mode of the LCD to display hard drive usage time instead of the temperature display using the SET button, the digit display (6) will show the number of days and hours the drive has been in use.

### **Fan Malfunction Display**

If the fan is disconnected or stops turning the thermometer symbol (5) will blink, the “alert” symbol (3) will come on, and an audible alarm will sound.

### **Temperature Alert Display**

If the temperature exceeds the factory setting of 130 degrees F, the screen will show the alert symbol (3). In addition, the thermometer symbol (5) will blink and an audible alarm will sound.

### **Programming the Temperature Alarms**

From the “Normal” display you can press SET to change the temperature display from Fahrenheit to Celsius. Use the up or down arrow buttons to make this change. Press the SET key again to confirm your choice and advance to the Temperature alarm threshold screen.

In the temperature alarm threshold screen, the threshold temperature blinks. Use the up or down arrow buttons to change the threshold. **Once you’ve set the desired temperature, hold down the SET key for at least 3 seconds to make the change permanent.** You should hear two beeps to indicate the setup is complete and the LCD display will return to “Normal”.

If at any time during the SET process you do not depress any buttons for 15 seconds, the unit will exit setup mode and return to the normal display. All settings made up to that point will be cancelled if this happens.

### **Silencing an Alarm**

If you hear a continuous alarm from your HR device, it means one of the following:

- One or more drive fans have stopped turning
- The temperature has exceeded the alarm threshold.
- The High-Rely alarm circuitry has malfunctioned.

Hit any blue button to silence the alarm. Then determine what caused the error condition and correct it.. Replacement fans and drive trays are available from Highly-Reliable Systems.

### **Safely Removing the Media**

To pull a drive out you will follow the steps outlined for inserting the drive in reverse but with one additional step. That step (step one) is to notify the PC operating system that the drive will be removed. The second part of the operation is to turn the key to “power down” the IDE hard drive. Finally you will remove the drive.

Although the newer Windows operating systems have an option that is designed to allow media removal without notification, to avoid corruption we recommend you follow this procedure until Microsoft



further debugs its USB removal code. Microsoft calls a USB drive removal without notification a “surprise removal” and has documentation about these removals on their web site.

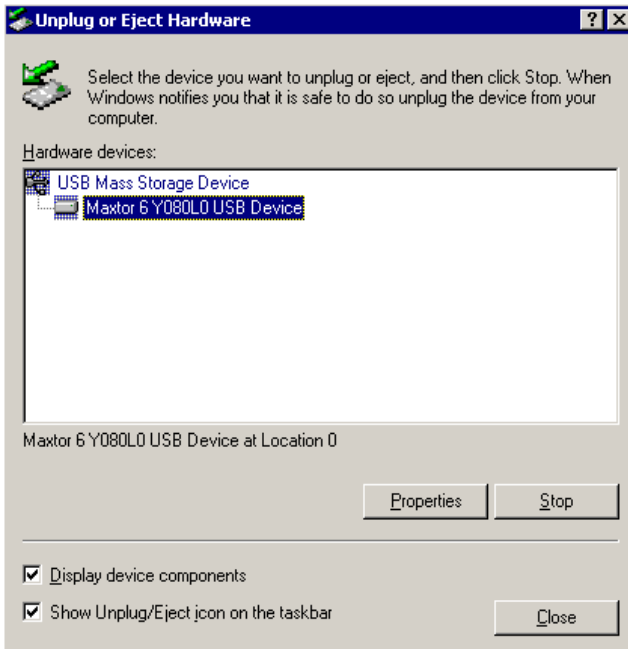
Start by logging into the server using the Administrator, backup operators, or other account with sufficient rights to deactivate hardware.

In the system tray (systray) of the desktop, (lower right corner of the screen), find the icon that looks like a small rectangular box with a green arrow floating above it as shown circled below. This Icon is the “Safely Remove Hardware.” Icon. If it is not there it may be hidden or configured not to display. You can alternatively use the Microsoft “Devcon” command as documented in the next section.



**Double Left-Click** on the icon. This should bring up a pop-up that states “Unplug or Eject Hardware”. Select the drive you wish to remove and left click “Stop”. You may see multiple devices associated with each USB device. Clicking any of the lines and selecting stop will notify the operating system of your intention to remove. Notice the two screen shots below look slightly different, which reflect two separate operating systems.





You should see the Safe to Remove Hardware bubble that states “The ‘USB Mass Storage Device’ can now be safely removed from the system”. If you get a message saying the drive is in use insure all running software including explorer windows have been shut down and try again. We have occasionally had software such as anti-virus or safe undelete programs prevent USB drives from being safely removed. If closing all programs doesn’t solve this issue you can consider rebooting the machine.



However, rather than rebooting a production server when this happens we recommend loading a process viewer to check what process is holding the USB drive letter open so that it can be shut down without delays or reboots. A free process viewer we have used successfully can be found at <http://www.teamcti.com/pview/prcview.htm>

As you can see from the screen shot below, the process viewer helps identify the drive letters and path that each running process might have open. Look for a process that is using the same drive letter as your high-rely drive and shut it down to allow safe removal.



Name	ID	Priority	Full Path
AcroTray.exe	2160	Normal	D:\Program Files\Adobe\Acrobat 5.0\Distillr\Ac...
BbDevMgr.exe	3000	Normal	D:\Program Files\Common Files\Research In M...
csrss.exe	880	Normal	H:\WINDOWS\system32\csrss.exe
ctfmon.exe	1792	Normal	H:\WINDOWS\System32\ctfmon.exe
DefWatch.exe	244	Normal	D:\PROGRA~1\SYMANT~1\SYMANT~1\DefWa...
DesktopMgr.exe	2392	Normal	D:\Program Files\Research In Motion\BlackBerr...
Explorer.EXE	3480	High	H:\WINDOWS\Explorer.EXE
Explorer.EXE	3884	Normal	H:\WINDOWS\Explorer.EXE
hkcmd.exe	1492	Normal	D:\WINDOWS\System32\hkcmd.exe
IEXPLORE.EXE	2288	Normal	D:\Program Files\Internet Explorer\IEXPLORE...
ieexplore.exe	2732	Normal	D:\Program Files\Internet Explorer\ieexplore.exe
inetinfo.exe	292	Normal	D:\WINDOWS\System32\inet_srv\inetinfo.exe



Notice in the upper right corner of the bubble that there is a small “X”. Single Left-Click on the X. (This confirms the change and will disconnect the High Rely drive from the system.)

Flip open the lock cover lever, Insert the key into the High Rely drive and turn counter-clockwise to power down and unlock the drive from the bay. You may now remove the drive from the bay safely by pulling open the release lever and pulling the drive straight out. Please refer to the drive removal section more specific instructions.



## Using Devcon to Safely Remove Drives

Microsoft has a command line utility called “Devcon” that is an alternative to using the graphical Disk Manager. This utility can also be used to create a batch file and a desktop shortcut for quick removal of all the USB hard drives in your system. This is especially useful for multi-bay High-Rely units as it allows one click notification to the operating system to stop all installed USB drives. Search Microsoft’s web page for knowledgebase article Q311272 for more information on Devcon. This article



also has a link to download the utility at no cost. We recommend you save the utility in %systemroot%\system32 or a similar location where the operating system can find it. %systemroot% is a variable that Microsoft uses to denote the folder the operating system is installed into. Normally this will be either c:\winnt or c:\windows. So in other words, for easy access on a typical Windows 2003 server you would save the utility in the c:\windows\system32 folder. On a Windows 2000 machine this would be c:\winnt\system32.

We recommend you create a two line batch file using notepad called “stopall.bat” with the following lines

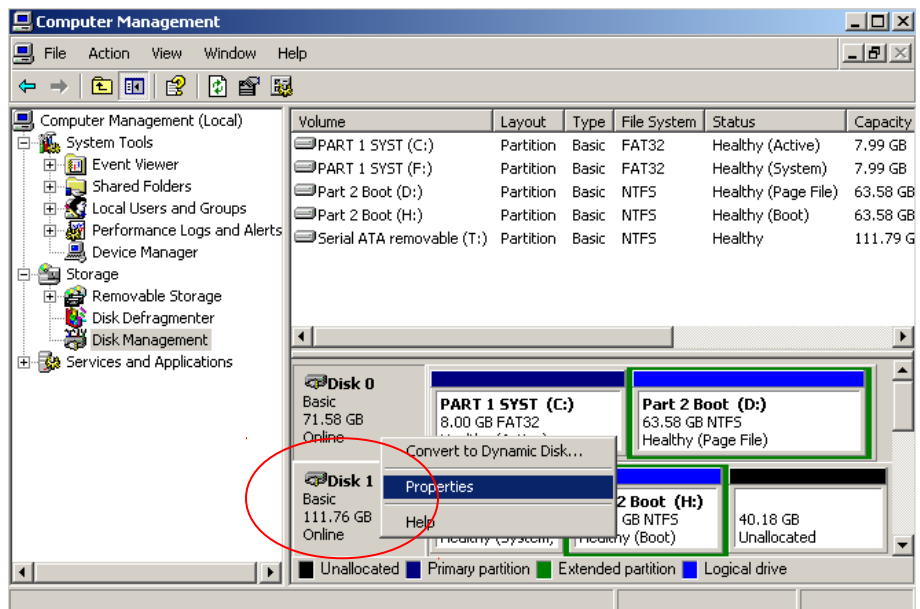
```
Devcon remove usbstor*
Pause
```

The only reason for the pause command is to allow you or your operator to see the result of the devcon command. Occasionally devcon will respond that it is unable to stop a device. Since it does not run in the graphical environment, the pause allows you to see what is happening before the window closes. Simply hit any key to close the CMD window and proceed to remove the drive(s).

If desired, it is possible to create devcon batch files to stop individual drives as well by modifying the parameters on the command line.

## A Note About the “Optimize for Quick Removal” Option

On the newer operating systems such as Windows XP and Windows 2003, there is an option to allow “quick removal” of USB hard drives. We believe you will find this option to be the default for USB drives but we recommend that you check the setting. To do so, right-click on My Computer, and select "Manage". Click on "Disk Management" in the left-hand column. Now Right click in the grey area where the “disk #” associated with your High-Rely displays. (See red circle in screen shot) and select “Properties”.



From this screen you will be able to select the “Policies” Tab. Note the radio button that allows you to indicate the drive should be “Optimize for Quick Removal”. The comment indicates that the setting



disables write caching on the disk and in windows so you can disconnect the device without using the safe removal icon.

We have used this feature with varying degrees of success. We remain concerned that even with this option turned on there are many occasions where selecting “safely remove” results in an error that the drive is in use and cannot be safely removed. We consider this to be a Windows issue and our advice is to err on the side of caution and always tell the operating system you are going to remove the drives even when you have this feature turned on.

Write caching a removable storage device is not recommended. Removing a disk without properly notifying the system can lead to data corruption. Data can still be buffered and not yet transferred to the disk when a disk is physically removed. Proper ejecting the disk through the system and system shutdown will allow the Windows disk administrator to transfer any unwritten data from the buffers and insure no files are open on the devices. If at any time you get a write cache failure that results in your data “disappearing from your HR drive please do not panic – Under certain conditions we have seen windows explorer erroneously show “empty” USB hard drives that actually had data. Upon reboot the data reappears.

*NOTE: Although we have confirmed that skipping the “safely remove” option can sometimes be done without data loss, we believe doing a “safe removal” helps insure that the drive is not in use, and will prevent data corruption.*

## Assigning Drive Letters on Windows Systems

By default, when you power on each HR media, it searches for the first free drive letter it can find. In a multi-drive high-rely system, it is possible that Windows will provide a different drive letter each time you power a given drive up, depending on what is free right then. One bay HR systems should not have this issue.

The order you turn the drives on determines which HR Media get what letters. This can cause problems, because backup jobs are typically set to write to a particular drive letter. (i.e. the Monday job writes to drive K:, the Tuesday job writes to drive L:, etc.). Additionally, there can be conflicts if you have mapped network drives already assigned to letters that the high-rely system thinks are free.

To handle the drive letter assignment issue you can:

1. Allow Windows to assign static drive letters to each drive but make sure to power each drive up in the same order each time.
2. Load and use the High-Rely Drive Manager software to re-map drive letters to your preferences. This software sits in the system tray and will detect drive changes and dynamically remap the letters assigned by windows based upon volume serial number. This way the drive letter will always be used by that media cartridge, so you won't have these problems. Please refer to the section below on HR Drive Manager for more information.

Alternatively If you prefer to use Microsoft’s “Disk Management” to change your drive letters, refer to the instructions below. However, you should be aware that if you change a drive letter on Media “A” to a letter (such as “N:”), pull the drive, put in media “B” and also label that drive “N:” you will find that



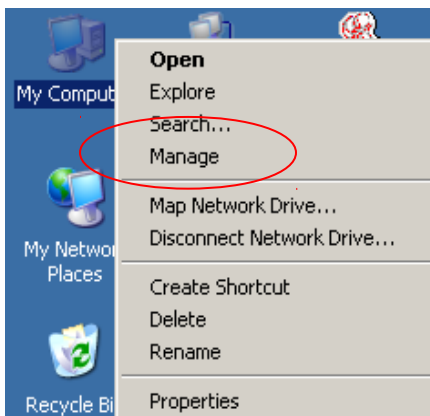
when you put the original media A back in the drive that it no longer retains the N: designation. This is a Windows problem that exists in all versions we have tried. This problem is worked around by the High-Rely Disk Management software.

## Assigning Drive Letters with Microsoft's Disk Management Program

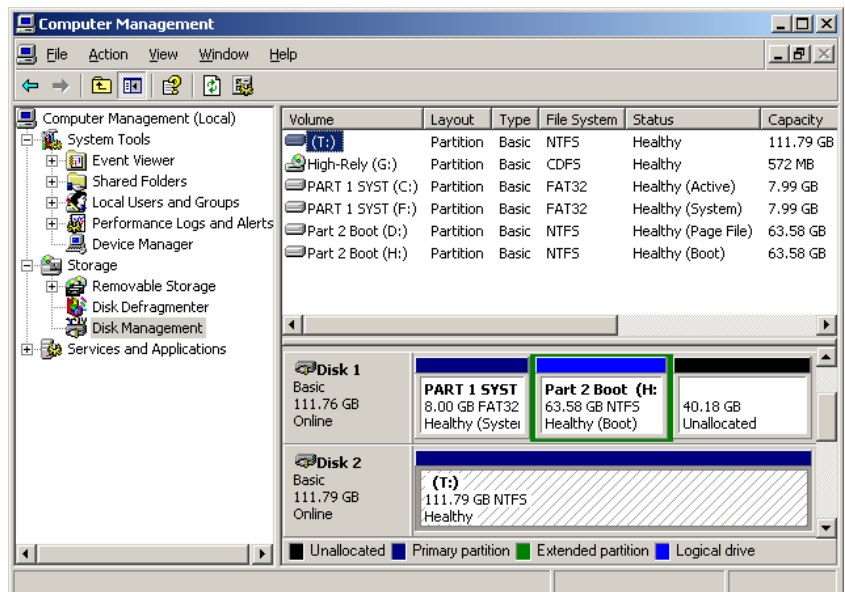
Before assigning new drive letters, you may want to record the "default" drive letters that Windows assigned each of your drives so that you can easily identify each drive. On single bay systems this is relatively simple – just note the drive letter as the unit comes on-line (Use the key to power it off if necessary). However, on multi-bay systems we recommend that you carefully power up one drive at a time using the key and record each drive letter and its associated drive bay position on the multi-bay unit.

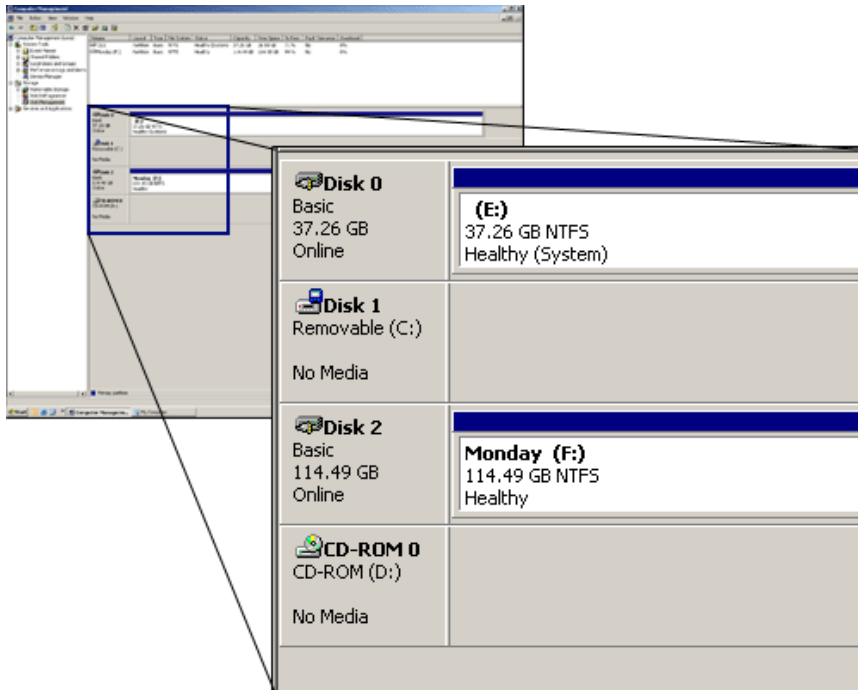
Once you've recorded the existing drive letters use Microsoft's disk management program to change them.

Right-click on My Computer, and select "Manage".



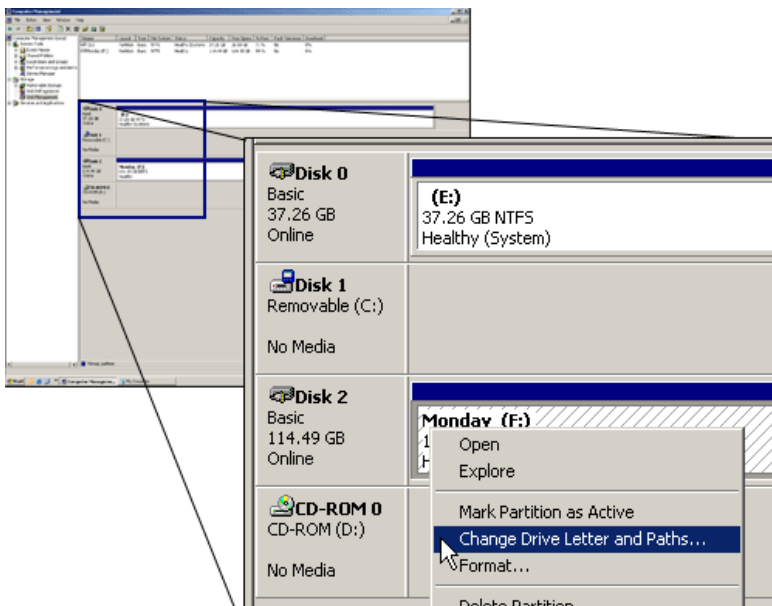
Click on "Disk Management" in the left-hand column. We will be Right clicking on the various drives and changing properties





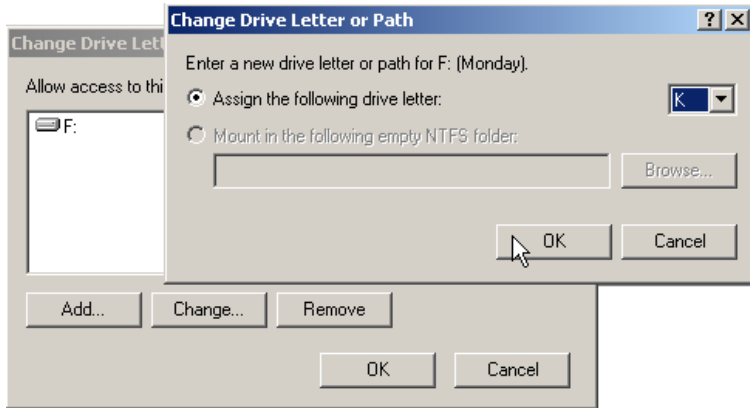
Notice in the above screen shot how the drive with volume label "Monday", has been dynamically assigned the drive letter F:. Let's say we want to change it to J:

Right-click on the volume "Monday", and select "Change Drive Letter and Paths", as shown below:



Choose "Change", and select the drive letter you want, then click ok, as shown in the next figure:

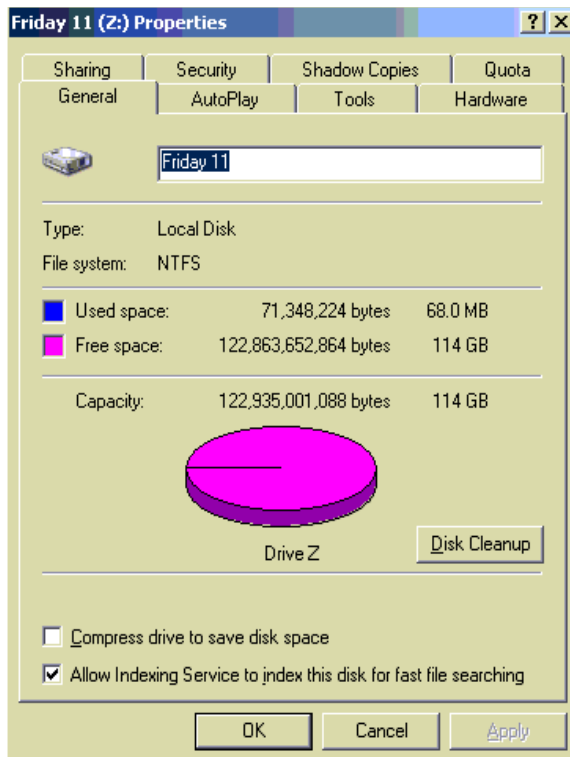




Repeat this procedure for every high rely media you have. Make sure all "Monday" media is assigned to one drive letter, all "Tuesday" to another, etc

### ***Disk Management Tips and Tricks***

You may want to consider turning off indexing for your High-Rely drives. We recommend this so that the operating system doesn't lock your drive without your knowledge, complicating the safe removal process. From disk Manager Right click on the primary partition manager portion of a given drive (right hand side that is usually white with blue band) and select properties. Uncheck the box on the general tab at the bottom that says "Allow Indexing service to index this disk for faster file searching". See the graphic below.



## Understanding the High-Rely Drive Manager

HR Drive Manager is a utility that runs under Windows 2000, 2003, Windows XP and Vista that solves some specific problems relating to drive letters in Windows operating systems. The software is not required to make the High-Rely drives work properly and you may safely use the High-Rely system without HR drive manager.

So what does HR Drive Manager do? Under normal conditions, when you plug any USB hard drive into any Windows system, the Windows OS will assign the next available drive letter to the USB device. For example, suppose you had a machine with one hard drive and one CD-Rom drive. These would typically be labeled C: and D: respectively. In this example, when you plug the USB drive in, it would be assigned the drive letter “E:” In some cases, you may find that there is a conflict with the Windows default drive letter assignment. This is particularly true when you have a multi-bay High-Rely device that uses a lot of drive letters. For example a 7 bay high-rely might use E:, F:, G:, H:, I:, J:, K:. It’s easy to see that one or more of these drive letters might conflict with existing drives or network mappings. For this reason, many people choose to “re-assign” the drive letters using Microsoft’s disk management software as described in the preceding section. However, there is a bit of a problem with the way removable drive letters are handled by Windows. Suppose that in the above example we reassigned the 7 drive letters to the “high end” of the available drive letters (T,U,V,W,X,Y,Z).

Windows will only retain these letter assignments until new media is inserted. So suppose you remove the 7 old drives (Set 1) and install 7 new drives. Windows will assign the new volumes E through K. Naturally, you will want to assign these 7 new drives (set 2) the same letter scheme as before (T-Z) so that the backup software will continue to use the appropriate drive letters and automatic backups will work properly. You can easily do this (again) with the Disk Management utility in Windows.

A problem may occur in “week 3” when you re-insert the original 7 drives (set 1). You may be surprised to find that Windows will label these drives E-K NOT T-Z. The reason for this is that Windows retains “memory” of only one volume associated with each drive letter for disks formatted as “Basic”. Since all USB hard drives must be formatted “Basic”, not “Dynamic”, we have provided the HR Drive Manager software. What the software does is automatically detect any USB High-Rely drive changes and map each physical hard drive to the appropriate letter based on a simple configuration (.INI) file. This text file retains data for ALL volumes installed in the High-Rely system indefinitely and always assigns the same drive letter each time that volume is installed.

### ***Installation of the High-Rely Drive Manager***

To install the software, you can launch it from the link on the autorun page of your High-Rely CD or double click the hrdm\_install.msi in the \High-Rely Drive Manager folder.

Name	Date Modified
InstMsiA.Exe	9/25/2001 12:05 PM
InstMsiW.Exe	9/11/2001 3:04 PM
Setup.Ini	5/17/2004 5:59 PM
hrdm_install.msi	5/17/2004 5:59 PM



## **Follow the on-screen instructions for installation of the High-Rely Drive Manager and consult the on-line help in the HRDM2 administrator when needed.**

### **The Backup Process – An Overview**

It is often said that one of the best ways for an administrator to loose his job is by failing to have critical data backed up when there is a hard drive failure. “Backing up” is the term we use when we make a copy of data stored on our hard drive. We usually copy our data to some sort of tape drive but the backup can be to other media as long as it meets the criteria for cost and reliability.

Hard drives are one of the few components in the computer with moving parts and tend to be subject to more failures than other parts of the system. Worse, almost any other failed component can be swapped out in a matter of minutes. When your hard drive fails, the data on that drive is lost and the time to repair is considerably longer. Making an extra copy every once in a while is an important precaution.

Backups can be a time-consuming and boring, and are a never-ending part of administering a network. It is rare that we spend so much time doing something we hope we’ll never have to use. Many administrators feel like the time they spend backing up is a wasted. Please don’t fall into that trap! While it may seem pointless to backup the same data over and over for years on end, you’ll be very glad you did when you finally experience a failure.

Many people assume that if they copy just their “critical data” onto a diskette, CD, or other removable media they are OK. However, you should consider the length of time to get your operation back up and running. It’s not uncommon to have it take several days by the time the drive is replaced, the operating system is re-loaded, and the software is re-installed. That’s why computer experts prefer to create a “full” backup of the entire system, including the Operating System. Think of this as like taking a snapshot of the data on your drive. The goal is to have a bootable image that can be restored to a new drive in a matter of a few hours or less.

In large firms, down time is measured in terms of thousands of dollars per minute or more. Ask yourself how long you can afford to be without your network and adjust the frequency and attention you pay to your backups accordingly. Obviously, smaller firms have a little more breathing room than administrators of “mission critical” computers in Fortune 500 companies have, but even small companies will want to have a disaster recovery plan that describes how to restore as quickly as possible. One of the single most important parts of your network “disaster recovery plan” will be your backup and restore strategy.

Studies have shown that human error—primarily accidental file deletion or modification—causes over one-third of all data loss. For the average business, whether a small, medium, or enterprise organization, the impact of lost data is at the least an inconvenience and at the worst a critical blow that can jeopardize



daily operations. The High-Rely system is superior to anything on the market for rapid restores on anything from a single file to an entire drive.

## How Hard Drives Work and Why They Fail

Many people have never seen an actual “hard drive”. In fact, one of the mistakes we have seen people make is to point to their computer (the CPU unit) and say something like “My Hard drive is acting up”. Actually, as figures 1-1 and 1-2 show, the hard drive is a little silver or black box somewhere inside the computer. It would be more correct to say “My CPU unit is acting up”

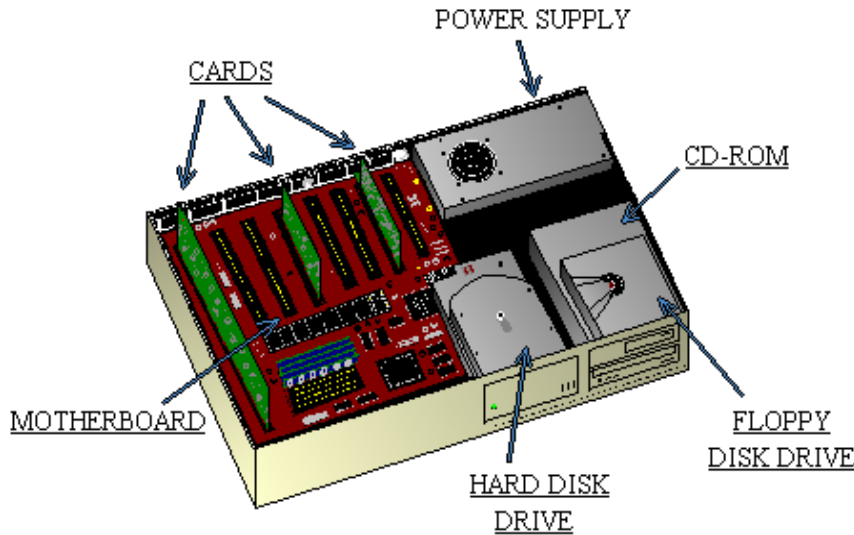


Figure 1-1 The Hard drive is located inside the CPU Unit

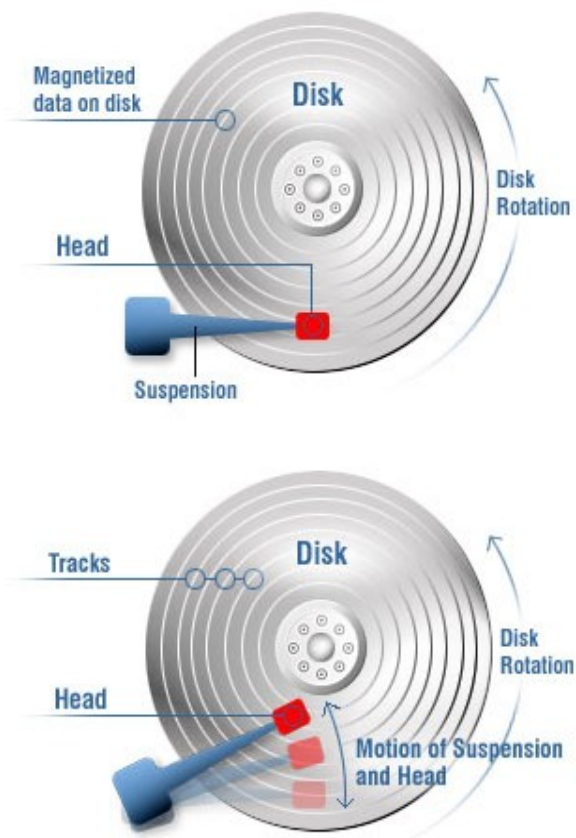
Figure 1-2 shows a hard drive with the top on and the same drive with the top removed (right). Hard drive manufacturers are fond of showing this removed top view, but it’s important to understand that the drive with the cover off has been ruined. Hard drives are hermetically sealed to keep out dust and dirt. One of the reasons is that hard drives fail is that the magnetic “heads”, which are supposed to fly very close to the surface of the drive, make contact too many times (or too hard) against the rotating platters, damaging the coating on the disk surface.



Figure 1-2 Inside the hard drive



Hard drives were originally invented back in the 1950's. Surprisingly, they haven't changed much since then in terms of their basic operation. The surface of the each rotating platter is coated with a material that can easily be magnetized. At the end of a small suspension arm, the drive manufacturer places a small electro-magnet. As the disk rotates, electricity can be passed through the head, effectively magnetizing a small spot on the disk. Like all magnets, these spots can be laid down in either a North/South or South/North orientation. As we lay down these spots, the path of the rotating disk under the head carves out "tracks" of data. These magnetic spots represent the binary zeros and ones that record all data inside the computer. The same head that writes the data can be used to read the data back because the magnetic spots induce a small electrical current in the heads.



*Figure 1-3 Rotating Platters Inside a Hard Drive*

### **The Importance of Retaining Multiple Backups**

Many people new to backup try to save money by limiting the number of backup media and reusing them on a regular basis. However this strategy can be "penny wise and pound foolish". It's important to realize that if backups are worth the effort it's also worth a small amount of additional effort and money to insure the backups are really good.

A scenario we've seen played out over and over again is variations on the following story: A corruption in the accounting database is first noticed in the Accounts Receivable module on Wednesday afternoon. The bookkeeper is doing what she normally does when the system gives her an error on the screen. But



it's late, the bookkeeper is tired and frustrated, so she shuts the machine down and goes home. Thursday is another day and the bookkeeper stays busy working on other tasks. By the time she gets back to the computer on Friday morning, she's forgotten all about that error. It turns out she works on Payroll Fridays and the AR system doesn't get touched until Monday. But Monday morning she gets the same error she saw last Wednesday and now she's in a panic. She's got an entire year's worth of data in this darn computer. Worse, she realizes something no one else in the office knows. She was put in charge of backups and has been using the same tape each night. After all, the tapes are expensive and she's always been diligent about saving the boss money. What all of this means is that the "bad" data has now been backed up over the last known good data several times. Not what we wanted!

It's an unfortunate fact that in most small networks, backing up data is given little attention. Another scenario we see is that a technician installs some sort of backup device, sets up a nightly backup schedule, gives someone in the office a quick overview on how to change tapes, and then leaves. Usually on the way out the door the tech reassures you that the backup will happen automatically. But there's more to a good backup than that! Inevitably what happens is that somewhere along the line the automatic backup stops working. Maybe the person trained to change the media quits. Maybe the media become dirty or the tape gets worn from repeated use. Perhaps some newly installed software conflicts with the tape backup schedule or the tape drive fails or someone in the office leaves their software running and the tape software dutifully "skips" the open files.

Whatever the reason, a lot of things can (and do) go wrong with backups! It's not enough to blindly shove the media in every day, trusting to fate that the software is working. You'll want to make sure to do it right and to view the backup logs after every session. We'll discuss those all important backup logs in more detail in an upcoming section.

It is critical to understand that automated backup must always be monitored to insure backups are working. It is very common for scheduled services to stop working for a variety of reasons. In addition, if users accidentally leave machines on at night the backup program will "skip" open files, resulting in the backup being useless for those particular files. Often these are the most important files in the mix.



## Top 10 Common Backup Mistakes

1. Tape Logs are not checked
  - a. It is critical to review the “log” files available in most backup software to see if files were skipped or other errors occurred.
2. Backup media not changed out each day.
  - a. Backups fail due to incorrect media or because previous job ejected tape.
3. User’s leave workstation logged in and critical software up on the screen at night
  - a. Most tape software will skip open files, which are often the most critical files in the enterprise.
4. Tape errors
  - a. Tapes have limited life and shouldn’t be used too often (50 or more uses generates errors on many tape sub systems)
  - b. Tape needs cleaning (dusty environments such as mines, construction sites, shops etc eat tapes quickly)
  - c. Tape Drive failures. Tape drives have a higher failure rate than most computer peripherals.
5. Customer doesn’t own the proper tape backup software that handles complex “always on” applications such as Exchange or SQL™.
  - a. For example, although the Native backup program that comes with windows 2000, 2003 or XP will backup exchange, but will not allow restoring individual mailboxes. Restore is an “all or nothing” proposition.
6. Relying on Incremental backups with unreliable tape media.
7. Customer believes that backing up just their data is enough
  - a. Truth is the time spent reconfiguring the operating system and reinstalling applications is often very costly.
8. Media not transported offsite on a regular basis.
  - a. Fire, flood, theft, employee malice etc can result in loss of critical data at the work site. It’s important to delegate someone to periodically remove a backup media (and bring back offsite media as needed.)
9. Failure to have sufficient media for a good history.
10. Failure to consider the need to archive
  - a. In today’s litigious environment, consider carefully whether you should retain emails or other important documents over a long period of time. This generally means “retiring” backup media permanently in an archive.



## Backup Software

Your High-Rely backup system can work with a variety of backup software programs. The software included with your drive is called “Backup Now!”. Backup Now! Is a very fast and flexible product that supports both High-Rely hard drive and DVD products.

Many tape drives vendors recommend or require special third party software to be totally effective. Although your High-Rely drives can be used with many of these same backup programs, we believe that the easy to use Backup Now! software that comes with your High-Rely drive and/or the NTBackup program that came with your Windows 2000, 2003, or XP operating system will work just as well in a variety of circumstances. You may find that using the native NTbackup program (which has traditionally been avoided by IT professionals) is more practical with a High-Rely subsystem than it was with tape. The reason for this is that the additional functionality of third party software is often rendered unnecessary by the speed, reliability, random access capability, and ease of use of the HR media.

Although we cannot support third party programs, we have provided some limited documentation on how to use the NTBackup program that ships with most versions of Windows. If you require advanced features such as sophisticated logging, backup of open databases or files, one step disaster recovery capability, etc you should definitely consider purchasing one of the many third party backup software solutions.



## Using Windows NTBackup

Your windows operating system comes with a built in backup program that can provide basic backup functionality with your HR media. This program is a “lite” version of an early generation product called backup exec currently being sold by Veritas. The program is essentially the same under the various versions of Windows including Windows 2000 (Professional and Server), Windows XP Professional , and Windows 2003. If you have XP Home edition please refer to the following section.

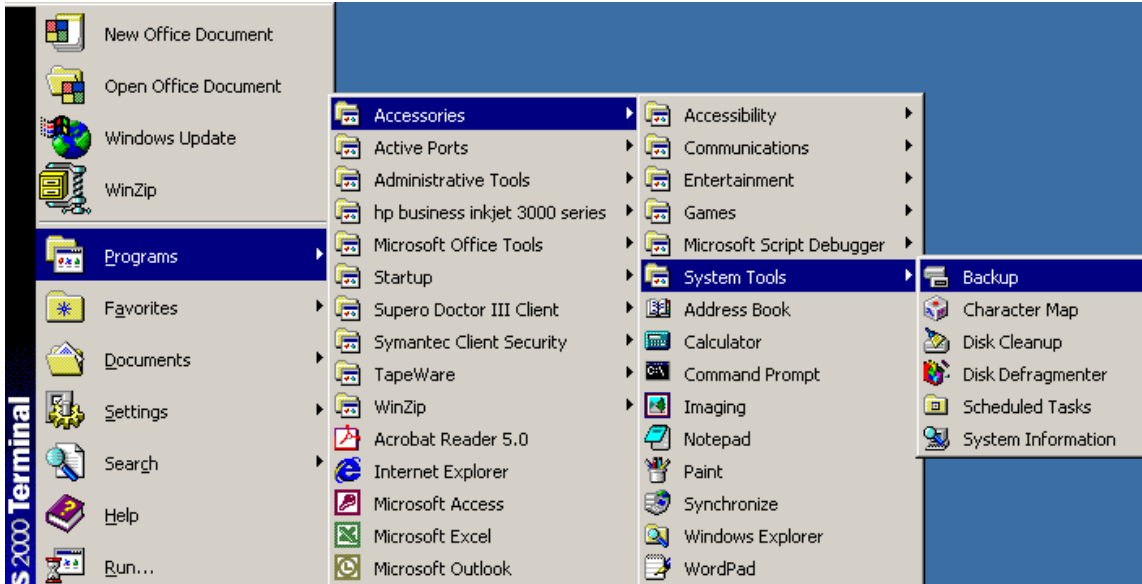
### A Note about NTBackup under XP Home Edition

XP Home editions don't install the program by default but you can find it under \VALUEADD\MSFT\NTBACKUP. There are some problems with the use of the backup utility with the XP Home edition. Apparently the NT utility's restore function does not work reliably with Home Edition's Simple File Sharing. Microsoft did not develop the backup utility (it is licensed from Veritas) and possibly did not want to invest resources in solving any compatibility issues before releasing XP Home. There is a very good discussion of the problem here:

<http://www.annoyances.org/exec/forum/winxp/n1040670211>



We will refer to the built-in backup program in the various versions of Windows as “NTBACKUP”. It can be found under Start, Programs, Accessories, System Tools Backup.

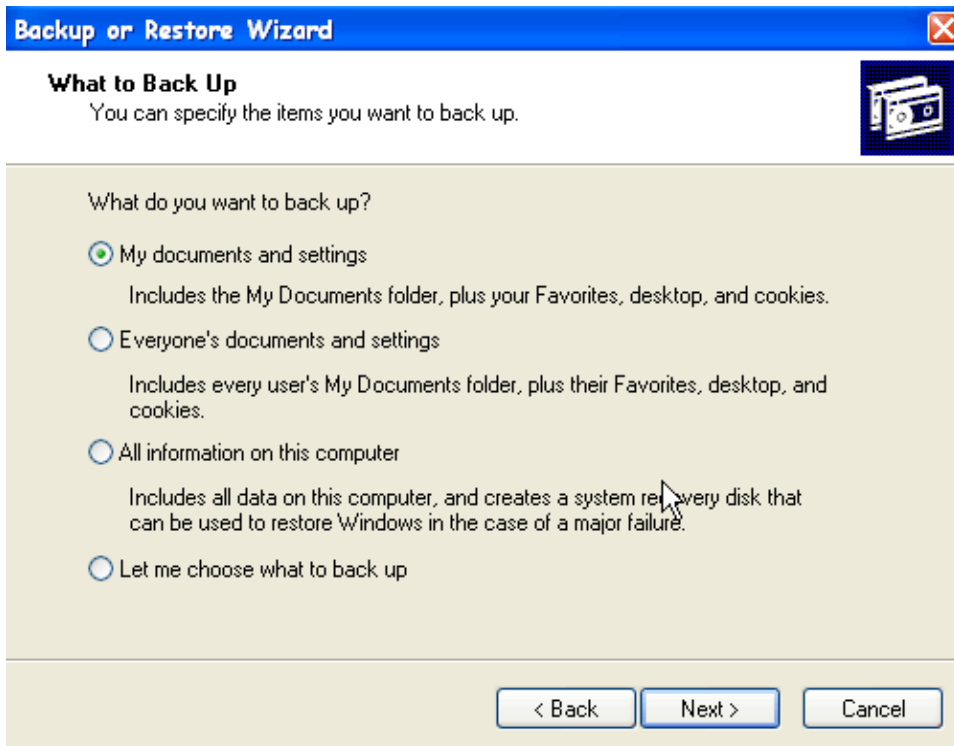


The NT backup program makes use of the Windows Schedule service to schedule periodic backup jobs. The backup wizard in the NTbackup software allows you to easily create backup jobs by walking you through the selection process. Alternatively, you can make backup selections and schedule your jobs manually. The following screens show Windows 2000 but the program is similar under XP and 2003.

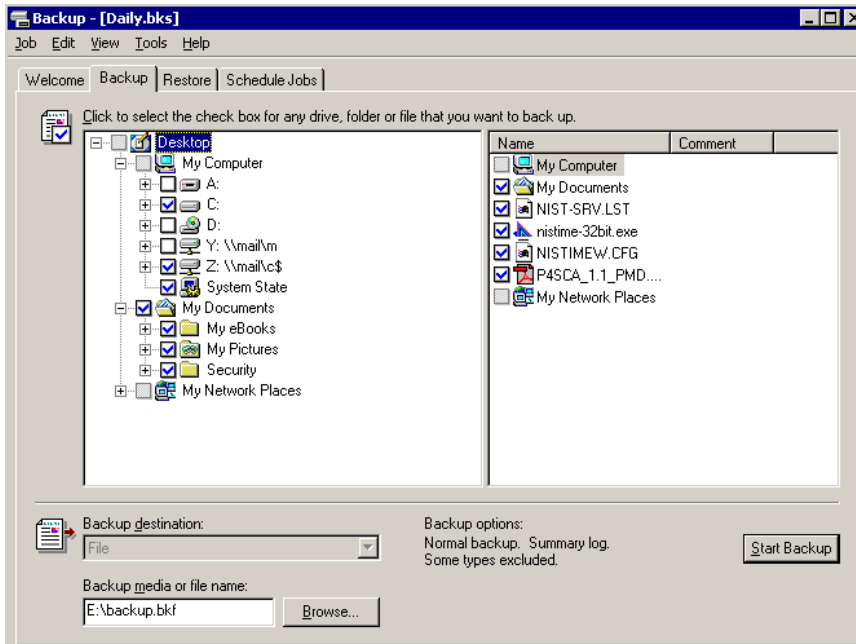


If you select the backup wizard the program will assist you in choosing what you want to backup. We recommend backing up everything including system state for most networks.





The Backup Selections can include both local and remote hard drives. However, keep in mind that a limitation of the built-in Windows backup program is that “system state” can only be backed up on the machine that physically has the backup device installed. System state includes critical operating system files required to restore your machine to a booting state in the exact same form it was prior to any outage. This limitation can be worked around by scheduling a “2 stage” backup (discussed later).



Notice that the backup destination will be a file (No other choices are allowed unless you have an alternate backup device in your machine such as tape). You specify the path and filename under the “backup media or file name” dialog box. Make sure to choose the drive letter associated with your High-Rely drive.

Often, you will overwrite this file each time you do a backup. Many clients choose to backup nightly to the same filename and then change the media that each backup goes to each day. This can be done by either swapping drives daily or, if you own a multi-bay High-Rely device by specifying different drive letters for different nights of the week.

You may want to consider whether your high-rely media will accommodate more than one backup. For example, if you have only 10GB of data to backup and your high-rely media is 80GB, you may want to create 3 to 5 individual backup jobs, each with their own filename and/or path. Each job would create a separate file on the drive, preventing the overwrite condition that would normally occur. The advantage of this is that you can store multiple backups onto the same media, providing a deeper history. Just be careful that the drive doesn’t get completely full with the number of backups you choose. Over time, your data set will likely grow and you want to provide headroom for that so backups won’t fail due to lack of drive space.

## ***Backup Rotation Schemes***

### ***XP Professional and Windows 2003 - Volume shadow copy***

Windows XP allows you to create shadow copy backups of volumes, exact point-in-time copies of files, including all open files. For example, databases that are held open exclusively and files that are open due to operator or system activity are backed up during a volume shadow copy backup. In this way, files that have changed during the backup window are copied correctly.

Shadow copy backups ensure that:

Applications can continue to write data to the volume during a backup.

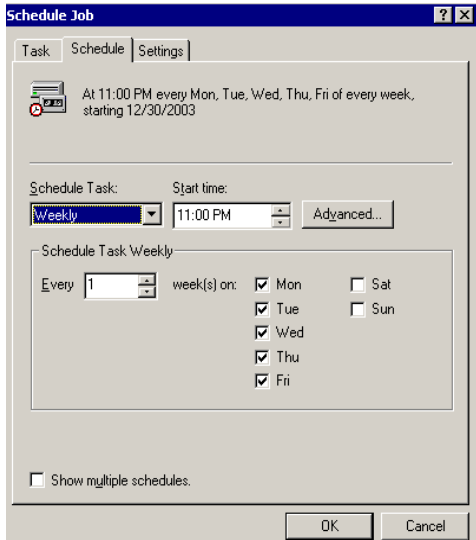
Files that are open are no longer omitted during a backup.

Backups can be performed at any time, without locking out users.

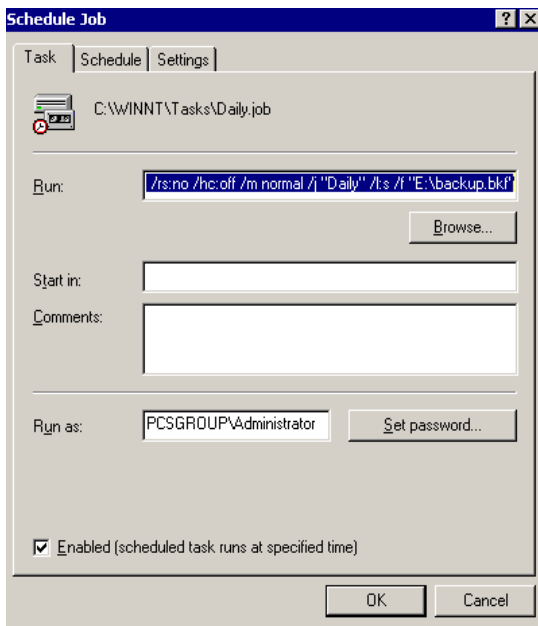
## ***Scheduling the Job***

Once you’ve selected the files you want to backup, you will want to set the options & backup schedule. The wizard will walk you through the schedule portion of the job. The simple configuration is to create a “weekly” job and then select the days of the week and time you want to run.



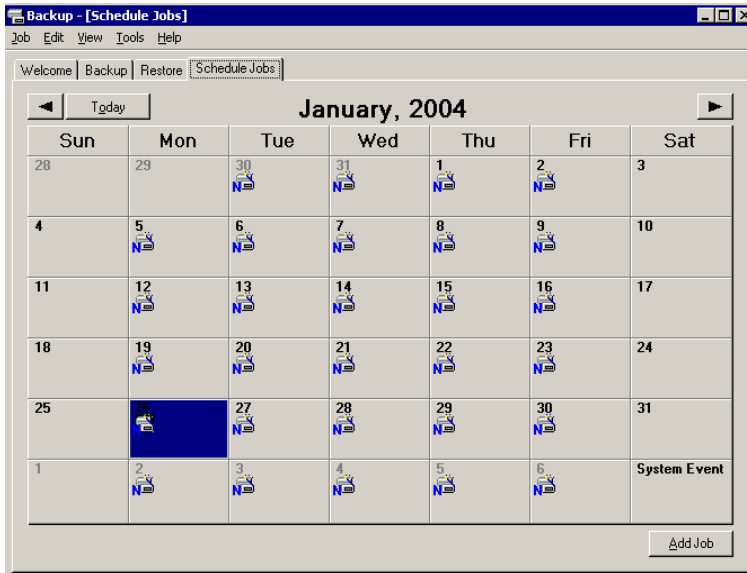


You should insure when you schedule a job that you run it in the “security context” of the administrator or another user that has sufficient rights to access all files. It is also important that this user does NOT have a blank password, as the scheduled task may not run.



The presence of an Icon on each day you want a scheduled backup to occur as shown below is an indicator that the job is scheduled.





## Backing up System State with NTBackup Two Stage Backups

If you would like to backup multiple computers to a single High-Rely device over the network using NTbackup, you should do a “two stage backup”. Although you can backup all data files across a network, NTbackup has a limitation that prevents certain files from transferring. This limitation is to encourage purchase of third party software that has more functionality. However, you can use the 2 stage backup as a workaround. This workaround also allows you to capture system state with NTBackup and then use Backup Now! For the second stage backup.

Suppose Server1 has the High-Rely drive and Server2 does not. The procedure generally involves using NTbackup on server2 to backup system state and any other information (such as Microsoft Exchange mailbox data), that can’t easily be backed up over the network sometime before the High-rely backup occurs. For example, you might tell Server2 to backup system state to a folder called “Server2\_systemstate” at 7pm each night. This backup by itself is not very useful because you will send the file to the same hard drive you are backing up. Thus, if you stopped here and had a hard drive failure on Server2 you would be unable to recover.

However, if you schedule NTbackup to backup both Server1 and Server2 at 9pm to the High-Rely device you effectively work around the limitation of the built in backup program by backing up the system state that was captured to the local drive on server2 at 7PM.

## NTbackup Review Checklist

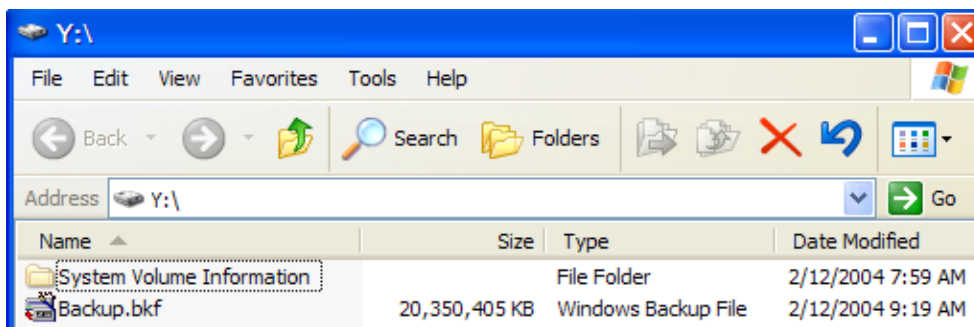
It is extremely important that backups be verified on a regular basis. Too many offices have diligently swapped backup media out day by day only to discover their backups were not restorable when a disaster finally struck. The following checklists detail some recommended “best practices” to insure your backups are good. In the following sections, we will describe in detail how to accomplish each of the following tasks.



- Verify the time and date of the backup file on the HR media matches the scheduled date.
- Verify the size of the backup is consistent with the size of the original data (compression may make values different)
- Review the backup report (log) for skipped files or other problems
- Note the backup speed and verify it is roughly the same as previous backups.
- Check the windows event viewer for errors that may have occurred during the backup process.

## 1. Reviewing Backup File Time and Date

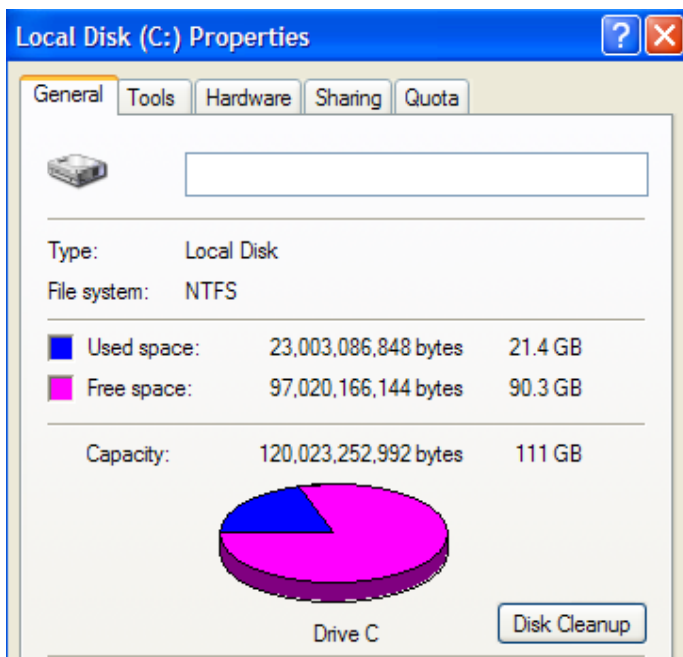
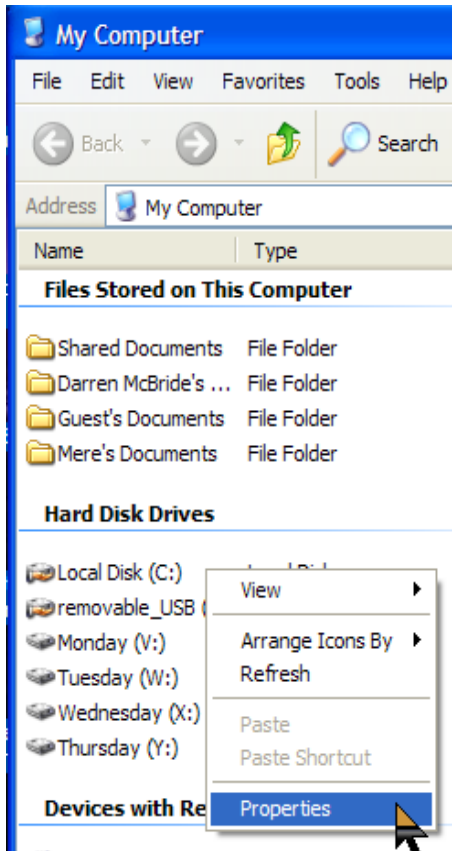
It is helpful to use explorer to confirm the date and time on your backup file on the HR media is what you would expect based on your schedule. If you are using the native Windows XP/2000/2003 backup, you can expect to see a single large file on your High-Rely drive. In the graphic below, we used “My computer” to open up the Y: drive and view the drive contents. Note the date and time on the “backup.bkf” file tells me when the job finished. You should make sure this time is consistent with when you scheduled your last backup job. You may also want to take note of the overall size (about 20GB in this example) so you can compare it to the size of the data (See step 2 of the backup verification in the next section).



## 2. Reviewing Your NTBackup Size

The second thing you should do to verify your backup is to compare the amount of data the backup program reports (or the size of the backup file when you view it in explorer as in step 1 above) to the size of the data as reported by Windows. Suppose you wanted to know how much data was on the C: drive of your machine. Windows explorer (or “My computer”) will give you this information by right clicking on the drive and selecting properties as shown below:

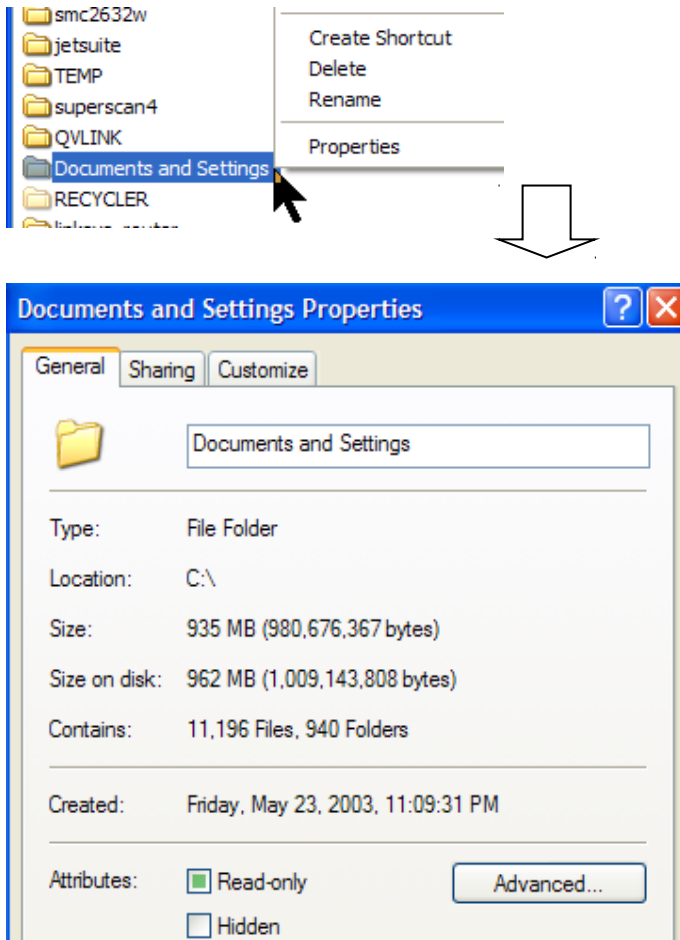




We can see that the above machine has approximately 21.4GB of data stored on the local C: drive.



In some cases your backup may encompass less than an entire drive. The same technique can be used to review total size of a given folder on the drive. For example, if you wanted to know how large your “Documents and Settings” folder was in preparation for a backup you could right click just that folder using windows explorer and select it’s properties as shown below to reveal that folder has approximately 962MB of data in it. This number should be compared against the size reported by the backup program after it completes. Although they may not be exact, the values should be fairly close to give you a comfort level that all your data is being backed up properly.

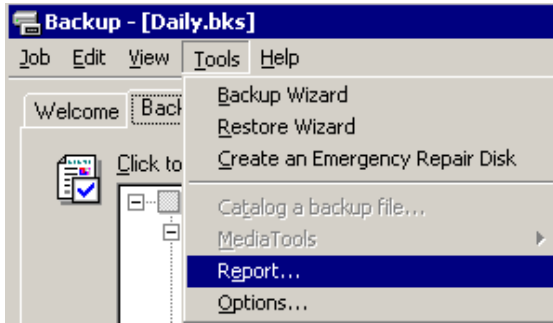


### 3. Reviewing the NTBackup Logs (Reports)

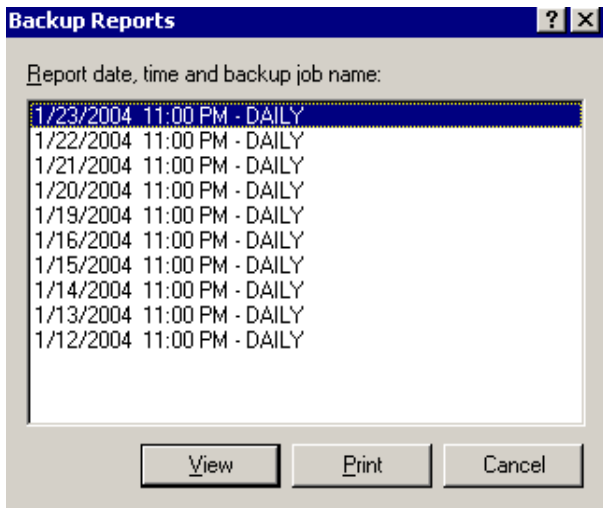
In addition to verifying that the size of your data roughly matches the size of your backup, it is critical that you review the results of your backup each day to insure the job ran and that files are not being skipped. The Windows NTBackup program creates what are called Logs or Reports to assist you in this review.

Backup Logs can be reviewed by selecting Tools, and Report from the NTbackup menu as shown below.



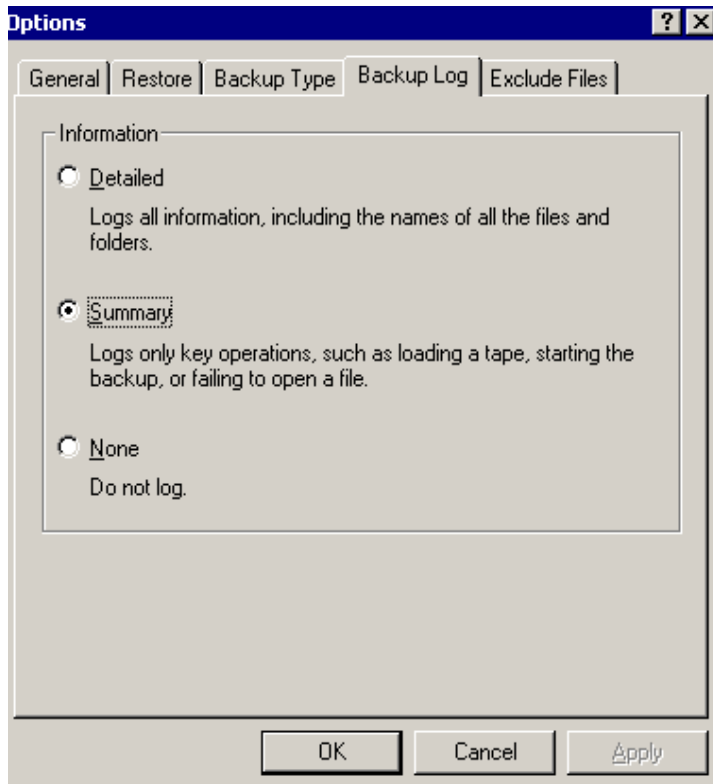


A list of reports by date and time will display for you to view or print



NTBackup uses Notepad to display the log. Depending on how much detail you selected for your backup, the log (under Tools, Options) may display all files backed up or only errors or exceptions such as files that were skipped. Normally, it is sufficient to set logging to “Summary” so that is easier to find only problem areas.





It is not uncommon to see files skipped on a server, although it is important to determine if the files are critical or not. Some OS files such as those associated with DHCP or WINS services as shown below will always be open and skipping them is not crucial to restoring your server. However, it may be a good idea to deliberately exclude them from the backup to make the logs easier to view and verify at a glance.

```
warning: The file \\WINNT\security\logs\scepol.log in use - skipped.
warning: The file \\WINNT\system32\dhcp\dhcp.mdb in use - skipped.
warning: The file \\WINNT\system32\dhcp\DhcpSrvLog.Fri in use - skipped.
warning: The file \\WINNT\system32\dhcp\j50.log in use - skipped.
warning: The file \\WINNT\system32\dhcp\tmp.edb in use - skipped.
warning: The file \\WINNT\system32\dns\dns.log in use - skipped.
warning: The file \\WINNT\system32\ias\dnary.ldb in use - skipped.
warning: The file \\WINNT\system32\ias\ias.ldb in use - skipped.
warning: The file \\WINNT\system32\ias\ias.mdb in use - skipped.
warning: The file \\WINNT\system32\msmq\STORAGE\QMLog in use - skipped.
warning: The file \\WINNT\system32\wins\j50.log in use - skipped.
warning: The file \\WINNT\system32\wins\wins.mdb in use - skipped.
warning: The file \\WINNT\system32\wins\winstmp.mdb in use - skipped.
warning: The file \\WINNT\Temp\JET229C.tmp in use - skipped.
warning: The file \\WINNT\Temp\JET3677.tmp in use - skipped.
Backup completed on 1/23/2004 at 11:31 PM.
Directories: 5619
Files: 54775
Skipped: 55
Bytes: 13,405,589,855
Time: 30 minutes and 33 seconds
```

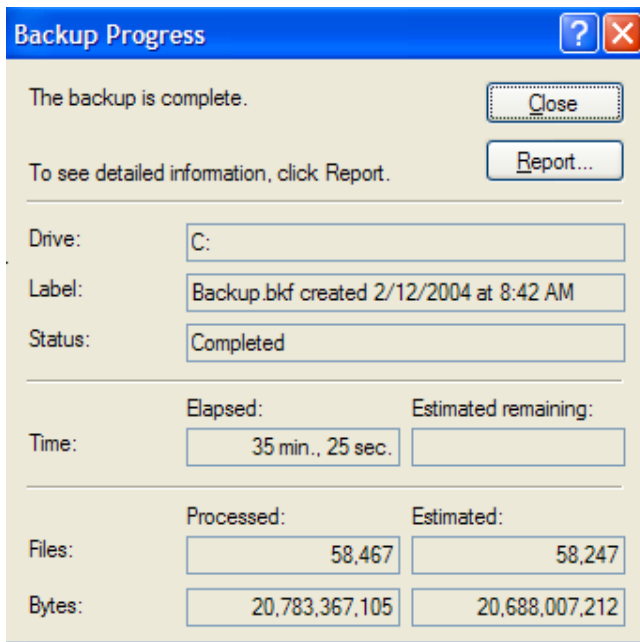


Other files, such as database or user files may be skipped because a user failed to log out of their machine and such errors should be discussed with users to avoid them. IT IS IMPORTANT to understand that files skipped will NOT be restorable and represent a substantial threat to a viable backup.

Entries such as those shown below may indicate a user failed to log out of the database and represent potential serious backup failures.

```
warning: The file \PCS_SHARED_INFO_&_COMMON\DOCS\Database\Repaired PCS Database.ldb in use - skip|  
warning: The file \PCS_SHARED_INFO_&_COMMON\DOCS\Database\Repaired PCS Database.mdb in use - skip|
```

#### 4. Reviewing NTBackup Performance



You can get the total number of bytes backed up and the length of time it took from either the final job completion window (if doing a manual backup) or from the “report” or backup log.

It is not a bad idea to keep track of the number of Megabytes per minute being backed up so that if the value changes you are tipped off to potential problems. Although the backup speed will vary somewhat depending upon the nature of the data, speed of the hardware, load on the machine/network during the backup, and other factors you should be able to “baseline” your backup speed and check it to insure it stays approximately the same each time.

In the screen shot above approximately 20 GB of data were backed up in approximately 35.5 Minutes. This translates to a backup speed of 559.59 MB/Min. You may do this calculation directly from the numbers shown above (20,783,367,105 bytes/35.42 minutes = 586769257.62 Bytes/Minute). Divide by 1024 twice to convert Bytes per minute to Megabytes per minute and you get 559.59 MB/Min. Multiply by 60 to get 33.6GB/Hr. We recommend you always convert to either Megabytes per minute or Gigabytes per hour for comparison purposes. You may want to consider logging this number so you can reference later if your backup changes speed.



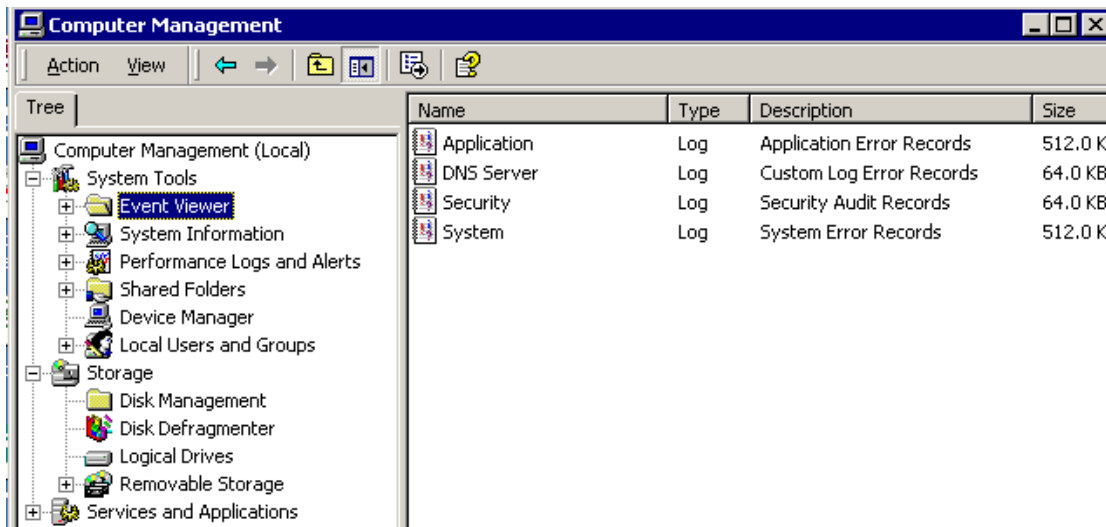
The above number was taken from a Pentium IV 2.8Ghz Running Windows XP NTBACKUP and backing up a local 7200RPM IDE hard drive via the USB 2.0 port. The data was sent to a 120GB 7200 RPM High-Rely backup media. You should expect to see slower speeds when backing up over a network or when backing up slow hard drives and slower machines with lots of smaller files. Expect faster speeds when backing up large files, using faster “sector level” copy software, or on machines with highly efficient USB ports

Over the network speeds will be considerably slower. 100MB networks produce on the order of 50MB/Min.

On a High-Rely system using the native Windows 2000 backup verify speeds are much faster than backup speeds. Unlike tape, which typically takes just as long to verify as to backup, verification of 10 or more times faster than the backup is possible. It’s not unusual to see your backup verify at over 1GB per minute.

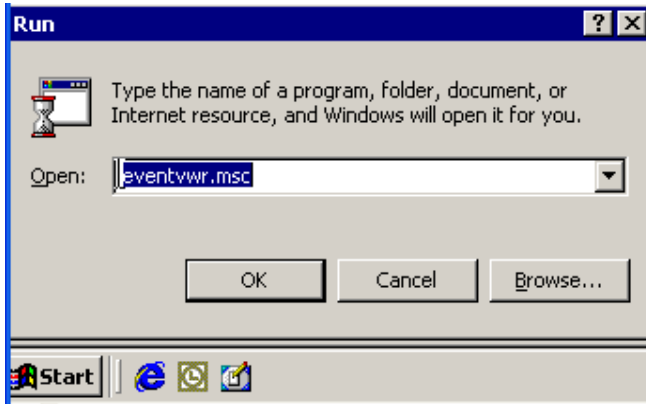
### 5. Checking The Event Viewer for NTBackup problems

It is important to review the Windows “event viewer” to see if the operating system is generating any errors or significant informational events during the backup process. Occasionally you will be able to see hardware problems or configuration problems that could indicate that your backup is not complete. To access the event viewer you can Right click on “My computer” and select “Manage”. You will see the event viewer as part of the management utilities. Using the events in Event Viewer, you can gather information about hardware, software, and system problems.



Depending upon your machine configuration you may also be able to find an event viewer icon under Start, Programs, Administrative Tools. Power users often get into the event viewer by clicking Start, Run and then typing in “eventvwr.msc”





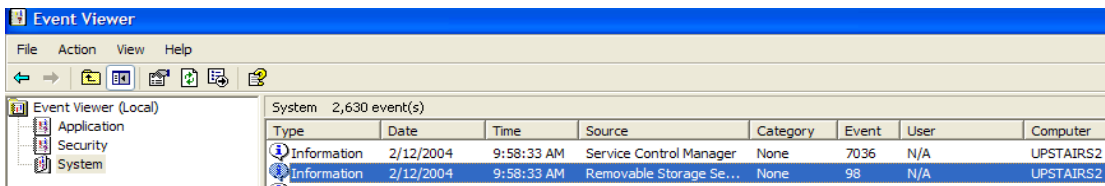
Windows 2000 records events in three kinds of logs:

**Application log** - The application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. The program developer decides which events to record.


**System log** - The system log contains events logged by the Windows 2000 system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined by Windows 2000.


**Security log** - The security log can record security events such as valid and invalid logon attempts as well as events related to resource use such as creating, opening, or deleting files. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log.

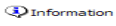
For monitoring backups probably the most important is the “System Log”. However, you will typically see at least informational events associated with the NTbackup program in the “application log”.



The Event Viewer displays these types of events:

**Error**  - A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an error will be logged.

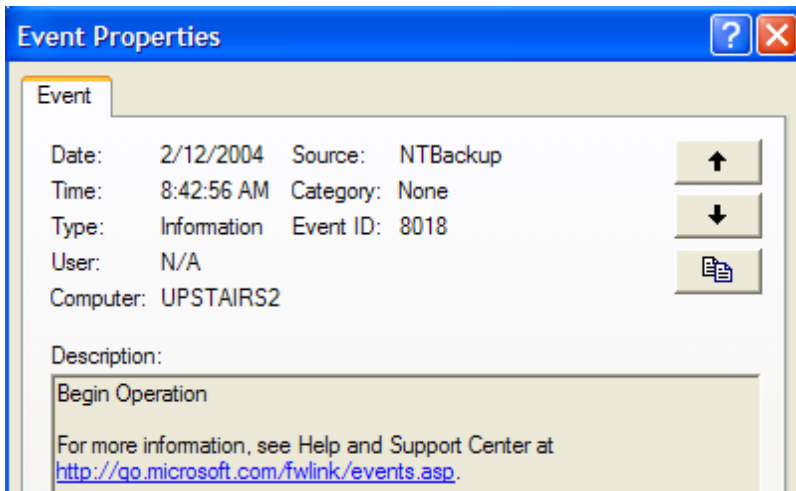
**Warning** -  - An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a warning will be logged.

**Information**  - An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.

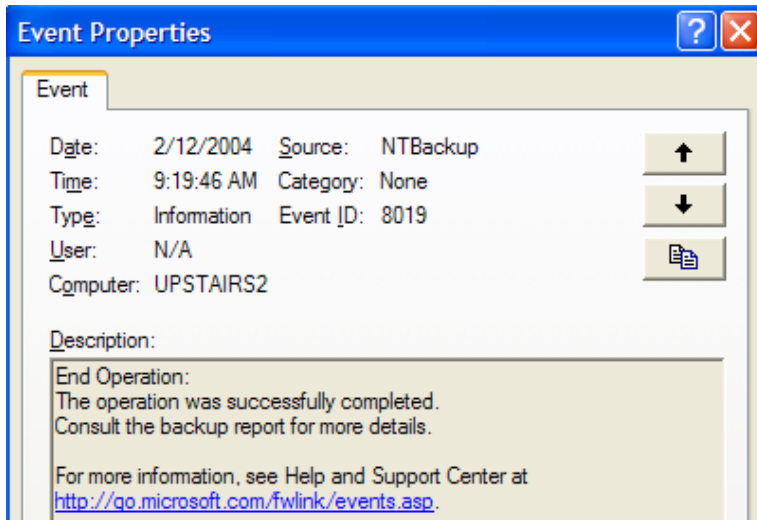


## Application Log

The application log is a good source for confirming a scheduled event such as a backup occurred. For example, you should see an event 8018 when NTBackup began its operation as shown in the graphic below.



Similarly, an 8019 event will be logged in the application log when your backup finishes. These times should essentially confirm those in the backup "report"



## System Log

You should focus on events that occur during the times you know your backup job ran. There are thousands of possible "events" that can occur and it would be impractical to document them here.





## Monitoring NTbackup

During the backup process the machine will be sluggish due to the amount of data being transferred. We recommend doing backups during off peak hours wherever possible. You can use the Windows task manager (accessed at any time by hitting Ctrl-ALT-DEL) processes tab to monitor the percentage of CPU and RAM usage the backup process is taking. As shown in the graphic below, the backup process is called ntbackup.exe. The cpu utilization as shown in the screen shot is 29%, meaning that 29% of the processor's time at this moment is being used by the backup process. This number will fluctuate widely during the backup process.

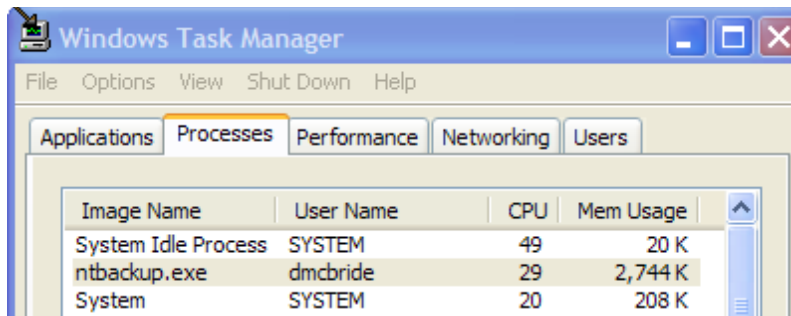


Image Name	User Name	CPU	Mem Usage
System Idle Process	SYSTEM	49	20 K
ntbackup.exe	dmcbride	29	2,744 K
System	SYSTEM	20	208 K

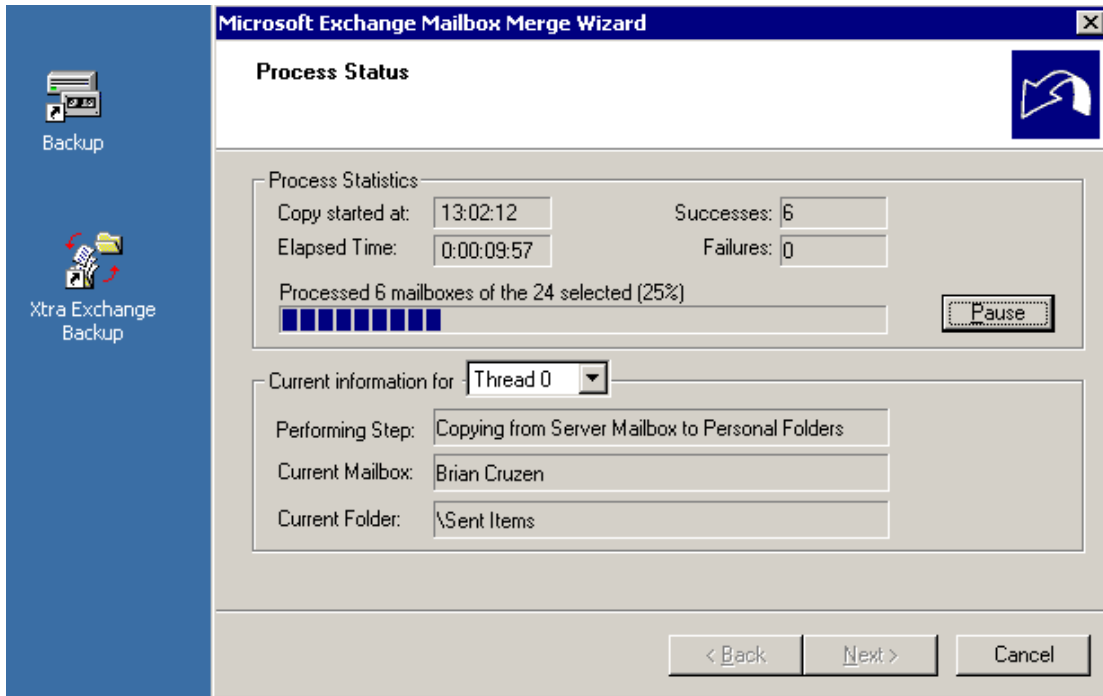
## Backing Up Microsoft Exchange with NTbackup

Exchange represents a unique challenge in that the service is “always on”. Traditionally, a file or database that is “open” during the backup will be skipped. To prevent a critical backup failure of mail Microsoft provides a mechanism to backup the “mailbox store” for Exchange servers. Basically, when Exchange is installed on a server an administration tool is added called the “System Manager”. Along with this tool comes a modification that allows NTBackup to “understand” how to backup open Exchange data stores. It is important to understand that this backup is “all or nothing”, meaning it is intended to restore the entire mail data set in case of disaster, but does not provide for backing up (or restoring) individual mailboxes or messages. This can be a problem in an enterprise environment where a critical e-mail is accidentally deleted. There is no way to recover this message without “rolling back” the entire mail store to the time of the backup. This could result in numerous other users losing messages received from that point forward.

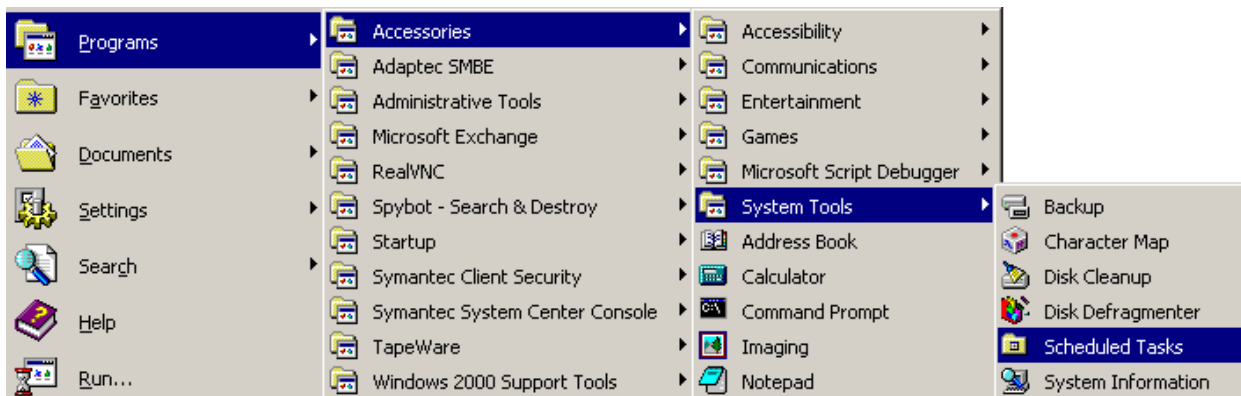
If this is a problem in your organization, you may wish to consider third party software alternatives such as Veritas Backup Exec or Computer Associates Brightstor that have Microsoft Exchange specific “agent” software available to do what is known in the industry as ‘brick level’ mail back up.



# An Alternative Exchange Mailbox backup Method



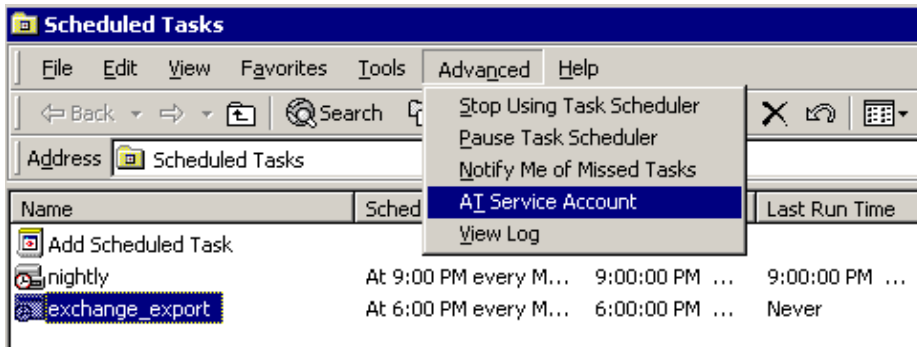
Because of the problem associated with restoring individual mailboxes as described above, if your organization does NOT have a third party backup product we highly recommend periodically exporting mailbox data out of the exchange database as an additional backup measure. Microsoft provides a utility to do this called exmerge that is included on the Exchange CD but not installed by default. Once installed and properly configured, a user with the proper rights can export individual mailboxes to a well known Microsoft mail format called a PST file. These files can subsequently be backed up to your highly media. Please refer to Microsoft's website and search for instructions on installing and using exmerge. The following screenshots demonstrate that the exmerge process can be automated and



scheduled.

This job is also scheduled to run nightly in Scheduled tasks





To insure that the job runs select Advanced, View Log. The results of the exmerge process can be viewed by looking at the following 3 files in the root of C:\

