Backup Export Tool

https://campus.barracuda.com/doc/78157267/

Data copies from a Barracuda Backup appliance to external media (tape or disk) using the Backup Export Tool. The Backup Export Tool is supported on Barracuda Backup 64-bit architecture firmware version 6.1 purchased after July 2012 and is available from the **System > Software Downloads** page in the web interface.

The Backup Export Tool, free for Barracuda Backup customers, allows Barracuda Backup users to export the historical revisions of data backed up and stored on a Barracuda Backup appliance or appliances. The Backup Export Tool is installed on a media server in the same network as the Barracuda Backup appliance. Once installed, users can browse connected Barracuda Backup appliances through the Backup Export Tool, locate data required for export, and export it to external media such as tape drives, tape libraries, virtual tape libraries (VTL), USB drives, and network attached storage (NAS). Data can be manually exported, or automatically exported on a schedule for weekly, monthly, and yearly revisions.

The Backup Export Tool was designed to allow users to export backup data to external media for long-term archival or for compliance reasons which may require data to be stored on tape or other form of external media. The Backup Export Tool is not intended to provide disaster recovery capability and exporting data from a Barracuda Backup appliance does not remove it from the appliance.

Export Data

Data stored "in-retention" on a Barracuda Backup appliance can be copied to external media for long-term archiving. This data includes file system data, application databases (Microsoft SQL and Exchange), and Hyper-V virtual disks, all backed up using the Barracuda Backup Agent for Windows. The Backup Export Tool can read "received" data from a Barracuda Backup appliance that is receiving data from another Barracuda Backup appliance in a site-to-site replication model.

Table 1. Frequently Asked Questions.

Which data types can be copied using the Barracuda Export Tool?	Data stored "in-retention" on a Barracuda Backup appliance can be copied to external media for long-term archiving including file system data, application databases (SQL and Exchange), and Hyper-V virtual disks. Support for VMware images available in version 6.3.01 and higher. *System-state and message-level data are not supported.*
Which types of external media are supported?	Tape drives, tape libraries, VTLs, USB drive, AWS Storage Gateway-VTL, and NAS.

Can data from Barracuda Backup be copied to tape or disk for disaster recovery?	When copying data from your Barracuda Backup appliance to external media, such as tape or disk, the data is first rehydrated (undeduplicated), then stored in the Barracuda Export Tool proprietary format. Data copies are for specific data types only and cannot be recovered back to a Barracuda Backup appliance if a disaster occurs. Configure Barracuda Backup to replicate to Barracuda Cloud Storage or another Barracuda Backup appliance to mirror the Barracuda Backup appliance data set for disaster recovery. In other words, if a disaster occurs, your data can be repopulated from the replicated copy.
How do I use the Barracuda Export Tool to copy data from a Barracuda Backup appliance?	The Backup Export Tool software is installed on a media server in the same network as the Barracuda Backup appliance. The media server must have access to the external media, for example, iSCSI adapter or via network shares. Data can then be manually or automatically copied to external media from a Barracuda Backup appliance. A report is sent once the job is complete by the Backup Export Tool software.
Can I encrypt data copies?	Yes, encryption is optional.
Which data revisions can be copied on a schedule?	Any revision can be exported manually. Only weekly, monthly, and yearly revisions are available for scheduled exports.
Is a separate subscription or hardware needed to use the Barracuda Export Tool?	No, there is no charge for using the Backup Export Tool.
Do I need to back up data using the Barracuda Export Tool and Barracuda Backup?	All data should be backed up using Barracuda Backup as your primary device for data recovery.
Can I use the Barracuda Export Tool with a Barracuda Backup "receiver"?	Yes, the Backup Export Tool can connect to a Backup "sender" or a Backup "receiver" for systems setup for site-to-site replication.
Will this interrupt my backup schedules?	No. Backups continue to run as scheduled. However, to improve performance, these can be configured to run at different times.
Is data purged off my Barracuda Backup appliance after it is exported?	No, data is not automatically removed from your Barracuda Backup appliance. All data on your local Barracuda Backup appliance is retained to match your configured retention policy.
Can I use the Barracuda Export Tool data copies with Offsite Vaulting?	Yes, the revisions you want to export using the Barracuda Export Tool must still be present on the local appliance. The Offsite Vaulting feature removes up to 12 monthly and 7 yearly revisions from the local appliance, keeping those copies in the offsite location.

How do I restore data from external media?	Once data is exported to external media, it can be restored back to the network using the Backup Export Tool. As the data is stored in a raw undeduplicated format, it can be recovered independently from Barracuda Backup.

Backup Export Tool Primary Server

The primary server hosts a special-purpose database, represented by the catalog object in the user interface. The database contains all information regarding the backup domain. The primary server is hardware agnostic, meaning it can be either physical or virtual.

System Requirements

Depending on your organization's backup needs, your system should meet the following requirements:

- The Backup Export Tool Catalog requires additional space. When you install the Backup Export Tool on the machine that will serve as the Domain Server, Barracuda recommends selecting a hard drive other than the default drive. A disk drive with at least an additional 20 GB is recommended
- VGA display with 1024x768 resolution, for use with Windows or an X Window System
- CD or DVD writer for use with the Backup Export Tool Bare Metal Disaster Recovery (recommended)

The Backup Export Tool supports all major storage hardware technologies and requires at least one storage media drive and/or library and the appropriate controller card.

- 512 MB RAM required (1024 MB RAM recommended) above operating system and application requirements
- 400 MB hard disk space required (typical installation)
- Internet Explorer 6 or higher required for all Windows installations
- At least 20GB hard disk space recommended on the machine that will serve as the Backup Export Tool primary server for the Backup Export Tool Catalog.

Supported Platforms

Barracuda Export Tool is supported by and has been tested with many different versions of Windows and Linux operating systems. For the most current list of supported platforms, visit http://www.barracudaware.com

> Barracuda recommends that you install the latest service packs and updates for your operating system.

Most operating systems list both minimum and recommended system requirements. As a general rule, if your system meets the minimum requirements for the operating system, it will also meet the minimum system requirements of the Backup Export Tool.

Barracuda has certified the operating systems and applications listed below to be compatible with the Backup Export Tool. The Backup Export Tool is designed using standard operating system facilities and has been observed to be compatible with more operating systems than have been officially certified. If your operating system distribution or version is not listed here, use the 60-day evaluation period to test Backup Export Tool in your environment.

Table 2. Windows Requirements.

Version	Edition	Proc	Service Pack
Server 2016	Standard	x86_64	
Server 2016	Datacenter	x86_64	
Server 2016	Essentials	x86_64	
Server 2012	Standard	x86_64	R2
Server 2012	Datacenter	x86_64	R2
Server 2012	Essentials	x86_64	R2
Windows 10	Enterprise	x86, x86_64	
Windows 10	Pro	x86, x86_64	
Windows 8.1	Enterprise	x86, x86_64	1
Windows 8.1	Pro	x86, x86_64	1
Windows 8	Enterprise	x86, x86_64	1
Windows 8	Pro	x86, x86_64	1
SBS 2011	Small Business Server	x86_64	
Windows 7	Home Premium	x86, x86_64	1
Windows 7	Professional	x86, x86_64	1
Windows 7	Ultimate	x86, x86_64	1
Server 2008	Foundation	x86, x86_64	2, R2 SP1
Server 2008	Standard	x86, x86_64	2, R2 SP1
Server 2008	Enterprise	x86, x86_64	2, R2 SP1
Server 2008	Datacenter	x86, x86_64	2, R2 SP1
Server 2008	Web	x86, x86_64	2, R2 SP1
Server 2008	Storage Server	x86, x86_64	2, R2 SP1
Server 2008	SBS	x86_64	2, R2 SP1
Server 2008	EBS	x86_64	2, R2 SP1
Server 2003	Standard	x86, x86_64	1, R2 SP2

Server 2003	Enterprise	x86, x86_64	1, R2 SP2
Server 2003	SBS	x86	1, R2 SP2
Server 2003	Storage Server	x86, x86_64	1, R2 SP2
XP	Professional	x86, x86_64	2, 3

Table 3. Linux Requirements.

The values in Table 3 apply to the listed versions—except Media Servers for tape, optical devices, and loaders—only in case of release kernel.

Version	Edition	Proc	Service Pack
RHEL 6		x86, x86_64	1, 2, 3, 4
RHEL 5		x86, x86_64	1, 2, 3, 4, 5, 6, 7, 8, 9
SLES 11		x86, x86_64	1, 2, 3
Ubuntu 13	Desktop and Server Edition	x86, x86_64	04
Ubuntu 12	Desktop and Server Edition	x86, x86_64	04[(1)], 10[(1)]
Ubuntu 11	Desktop and Server Edition	x86, x86_64	04, 10
Ubuntu 10	Desktop and Server Edition	x86, x86_64	04, 10
Ubuntu 9	Desktop and Server Edition	x86, x86_64	04, 10
Note: [(1)] Bare Metal Disaster Recovery (BMDR) is not supported with 3.5.x kernels.			

Encryption and Compression

Encryption is the process of changing data into a form that cannot be read until it is deciphered, protecting the data from unauthorized access and use. Company policy normally determines when encryption is required. For example, it may be mandatory for company confidential and financial data, but not for personal data. Company policy will also define how encryption keys should be generated and managed.

The current version of the Backup Export Tool provides the user with the ability to encrypt the data that is written to the media and fully implements the Advanced Encryption Standard (AES) for both hardware and software encryption.

- Hardware encryption is supported on some backup devices, such as HP LTO-4 tape drives. It is faster than software encryption and requires no processing on the backup server. The encryption strength is determined by the backup device. HP LTO-4 tape drives always provide strong AES-256 encryption. This feature can be managed by a backup application that supports hardware encryption, such as the Backup Export Tool.
- Software encryption uses the encryption algorithms available within the Backup Export Tool.

The user selects an encryption strength: Low 56 bit, Medium 128-bit or High 256-bit. Each encryption key size causes the algorithm to behave slightly differently. Increasing software encryption strength makes the data more secure, but requires more processing power.

If your business requires you to use encryption, the Backup Export Tool allows you to set the required encryption types and levels.

Cryptographic Algorithms

Cryptographic algorithms are the basic components of cryptographic applications. It is important to understand that as you increase the complexity of the encryption the information gets closer to impossible to read and the load on your machine, for software-based encryption, will increase.

Table 4. Software and Hardware Requirements.

Requirement	Description
Software	Three cryptographic algorithms are provided. These three settings provide three levels of resistance which require progressively more CPU time to convert the same amount of data. The three options are for the software encryption mode only. • **Low** – DES 56-bit • **Medium** – AES 128-bit • **High** – AES 256-bit
Hardware	The cryptographic algorithm provided by hardware devices that provide this feature is not under the Backup Export Tool control. The hardware provides configuration and operating parameters via a special encryption command. The device driver adjusts its crypto session settings from this input. Hardware encryption is an on/off feature, you do not have the ability to adjust the encryption level through the Backup Export Tool interface. By default the Backup Export Tool attempts to use the highest encryption algorithm supported on the device, if the device supports multiple algorithms. If the device does not support encryption, the user will be prompted with an alert telling them that the device cannot be used since it does not support hardware encryption.

Passphrase

The passphrase is a series of characters that must be provided by the user for input to the cryptographic key generation process.

- Passphrases must be no less than eight logical characters. They may be created by the user or randomly generated by a separate application.
- If created by the user, the passphrase should be difficult to guess and should contain a mix of lowercase/uppercase letters, digits and special characters.
- The passphrase is one of the components the Backup Export Tool uses to generate the encryption key. A longer or random passphrase will increase the strength of the encryption key even more.

- To aid the user in remembering the passphrase, the user may enter a hint message. The use of this field is optional and provided to the user as prompt for remembering the passphrase.
- If a backup job spans multiple media, the same passphrase will be used for all media in the set.

Passphrases for the media are stored in the the Backup Export Tool catalog. This means the user is able to read and append to the encrypted media without being prompted for a passphrase as long as it is being accessed by the instance of the Backup Export Tool that first encrypted it.

Once a media is deleted or exported from the Backup Export Tool catalog the passphrase is also deleted. There are two instances when the user needs to know the passphrase:

- When importing the media to another machine or another instance of the Backup Export Tool
- During disaster recovery

Important
Managing the passphrase is a critical component of any encryption system. Data may be stored for months or years, so passphrases must be archived securely. The user should keep a record or backup of encryption passphrases and store them in a secure place separate from the computer running the Backup Export Tool. If the user is unable to supply the passphrase when requested to do so, neither the user nor the Backup Export Tool Support can access the encrypted data.

Encryption Options

Encryption is enabled on the job's **Encryption** page.

Table 5. Encryption Options.

Option	Description
Off	Both hardware and software encryption are disabled.
Automatic	This selection uses hardware encryption if it is available from the device; otherwise, software encryption is used.
Software	Software encryption is used. When **Software** is selected, the user can choose the strength of software encryption.
Hardware	Hardware encryption is used if the device supports it. If it does not support encryption and this option is selected, the user is prompted with an alert stating that the device cannot be used since it does not support hardware encryption.

Software Strength	Options for the software encryption strength are listed below as three selections, low, medium and high. **Low** is the easiest method to decipher by outside methods, **High** is the hardest method to decipher by outside methods. As you progress from low to high, the encryption algorithm requires more CPU computations for each block of data to be encrypted, which may slow down the data stream to the device and increase CPU loading on the Media Server.
Encryption passphrase / Verify Passphrase	The user-supplied portion of the encryption key. The Backup Export Tool uses this value, along with other information it generates, to calculate an encryption key for the media. The passphrase must be entered twice to minimize the change of making a mistake while typing.
Hint	The text entered here is added to the log file of an import job if the media later needs to be imported and the incorrect passphrase is supplied. Use this field to create a reminder of the passphrase as the Backup Export Tool cannot recover a lost passphrase.

Key Management

The Backup Export Tool has adopted a very simple key management strategy. A media is encrypted originally by configuring the job that creates it according to the parameters described above. From that point on, the media is known to the catalog. As long as the media is known, restore jobs may use the media without entering the passphrase again. If a media is unknown—because it was deleted from the catalog or because it came from a different catalog—you must import the media to make it known to the catalog again. The import process required you to supply the passphrase to complete the import. If the passphrase supplied does not match that used to encrypt the media, then the hint supplied at encryption time is shown in the job log so you can try the import again.

When media is encrypted the media is depicted on the **Jobs and Media** view with a lock on it. The Platinum colored lock indicates hardware, and the gold lock indicates software encryption. The Media details window shows the type of encryption used.

Compression

Software encryption disables hardware compression, although you will still be able to select **Software compression**.

If the backup device has hardware compression then performance is better if only hardware compression is used, and that there is little to no benefit of having both enabled. Enabling software compression in this circumstance reduces performance.

If you select **Hardware** encryption, Barracuda recommends that **Enable hardware compression** is also selected. Hardware encryption and hardware compression can be used on devices, such as the HP LTO-4 tape drive, without any loss of backup speed.

Backup Schedule Settings

You can define retention policies which allow you to balance your data protection and historical retention needs with the economic realities of media and management costs. To determine the type of backup job to create, answer the following questions:

- How many days of data can you afford to lose?
- How large will a full backup job be?
- How much does your data change on a day-to-day basis?
- How many media does your budget allow?
- How much data can the backup media hold?
- If you have a library, how many tapes does it hold?
- Are there times when your tape drive will be unavailable?
- Will the amount of traffic on your network require backup jobs to be scheduled to run during non-peak periods?
- Are there certain days of the week when running lengthy jobs will interfere with other uses of your network?

Scheduling Concepts

Typically it is not practical from either a time or a media perspective to create a full backup every day. The solution involves running different types of jobs (full, incremental, differential, or copy) on predefined schedule intervals using predefined numbers of media sets that are reused over time. The process of reusing media is referred to as media rotation. The media rotation type determines how and when each media set is used, how long it is retained once it contains data, and the granularity of your backup history.

Table 6. Scheduling Concepts.

Concept	Description
Media Sets	The Backup Export Tool organizes media into sets based on the rotation type and schedule interval. Whether the job requires several or only one physical media to complete, they are identified in the Backup Export Tool catalog as a set. When more than one physical media is required for a job, the Backup Export Tool creates a unique name for each media in the set. When planning scheduled backup jobs, it is important to know whether one or several physical media are required to complete a backup job. This can usually be estimated by comparing the size of the backup selection to the capacity of the selected media. If you do not want the Backup Export Tool to use more than one media for a backup job, then you must select fewer files to back up. The term media can be used to refer to both physical media, like an LTO tape, or to the catalog object the Backup Export Tool uses to keep track of file versions.

Intervals	Job schedules are defined using the Intervals Daily, Weekly, Monthly, and Yearly. Intervals are used to define which days a job runs, the type of backup (full, incremental, differential, or copy), and how many sets of media are dedicated to the interval. The size of an interval refers to the amount of time between interval runs. When the Run repeatedly schedule type is selected, the job Configuration page displays an additional section, Interval settings, that controls the schedule parameters. Each interval type is listed along with a textual description of its current setting. To customize interval settings, click on the interval button. Most schedules are defined in terms of the following intervals: • **Daily** – Run on sequential weekdays. • **Weekly** – Run once per week on the day specified by the user, for example, Friday. • **Monthly** – Run once per month on a day specified by the user such as the first day, the last day, the first Monday, and others. You can also specify how many months should elapse between monthlies. Setting the monthly interval to every 3 months creates a backup every quarter. • **Yearly** – Tun once per year on a specified day of the year. By increasing the interval you can also schedule a job to run once every so many years. There are also **Hourly** and **Minute** intervals that are less commonly used. The concepts behind using these are similar to those of the intervals discussed above. For all intervals there is a setting that controls the number of sets. This setting determines how many sets of that backup interval are created before the Backup Export Tool goes back and overwrites the first. For example, if your schedule starts in January and calls for three monthly sets, you will have a set for January, a set for February, and a set for March. In April, the job will overwrite the set from January. When configuring a rotation the Calendar view displays the schedule graphically. The interval type for each day is displayed in the calendar. Click on a day in the calendar to display the type of backup, the write mode, and the name of the media that is to used on that day. Right-click on a day in the calendar to change the schedule interval for that day. This is useful to prevent a job from running on a given day. This is helpful for times when you know the job will not complete because you are unable to supply the right media for the job, as in the case of holidays. Click the name of a day in the calendar view heading to enable or disable jobs from running on specified days of the week. For example, if you want daily backups on Saturdays.

Implications of Intervals for Restoring Data	Intervals also define the granularity of the data you can restore. Rotations are set up to capture more granularity in the recent past and less granularity as data gets older. Larger intervals, like Yearly and Monthly, produce lower granularity data history. Smaller intervals, like Daily, produce higher granularity history. Take, for example, a rotation with three full monthly backup sets on the last day of each month, four full weekly backup sets created on each Friday, and four incremental daily backup sets created Monday through Thursday. Now suppose you have a critical file that changes daily. On Wednesday, you are asked to retrieve the file as of a specific date. With this rotation you can roll back to the Monday and Tuesday versions of the file in the current week and the Wednesday, Thursday, and Friday versions of the file in the previous week. Beyond that, you will only have the versions of the file as they existed on Friday for the previous four weeks previous to the current week. And beyond that you will only have the versions of the file that existed on the last day of the month for the previous three months. The catalog keeps track of the files and versions that have been backed up so you do not have to remember what media they are on. This knowledge makes the restoration process very simple. You only need to specify the files you want restored and the Backup Export Tool prompts you for the media it needs to restore the files. Full reconstruction of data may require multiple media sets. For example, to reconstruct the data for a Wednesday from a GFS 20 set rotation type, you will require the full backup media set from the previous end of week and all of the incremental media sets from that week (that is, Mondays, Tuesdays and Wednesdays). In some circumstances, the preceding full backup media set will be a monthly or yearly job and not a weekly job. As long as none of these media sets are overwritten, full data recovery is possible. When a full backup media set is reused, any incremental or differential backups relative to that full backup are no longer usable for full system restores. However, files on those media are still recoverable. Yearly backups only provide you with access to files present on your computer or network on that one day each year. No copy exists for files that were created after the oldest yearly backup and then deleted before the most recent yearly backup. It is the responsibility of the user to manage the retention of media containing critical business data.

Media Rotation Types

The Backup Export Tool provides several default media rotation types. These types can be used as is or as examples for creating custom rotations.

> Each media set may contain more than one tape or media. Several factors determine how much media you will need: the type of backup being performed (for example full, differential, incremental), the amount of data to be backed up during a full backup, and the media's storage capacity. If the total size of a full backup is larger than the capacity of the tape, additional tapes are required. Your historical usage is the best guide to determining how many tapes these jobs will require.

Table 7. Media Rotation Types.

Media Rotation Type	Description
No Rotation Type	When no rotation type is selected. the user may schedule the days to run on but the Backup Export Tool does not manage the media. The user must supply the desired tapes each time the job runs and manage the reuse of older media.
Fixed Rotation Type	Media sets are named for the interval that has been run, and follow the form *[Interval]* Set *[number]* • **Fixed by day of week** – For example, a daily media set is *1st Monday* • **Fixed by week of month** – For example, a weekly media set is *1st Week of the Month* • **Fixed by day of month** – For example, a monthly media set is *1st Month* An example of yearly media set is *Yearly 1* • **Fixed by day of year** – For example, a yearly media set is *First Day of Year 1*
Daily Append	This is a special rotation designed for users with a single backup device. It is the only rotation that appends data to media. It performs a full backup on the specified day followed by daily incrementals on the remaining weekdays. At the end of the rotation, the user must insert new media for the job to use. This rotation assumes that an entire week of backups will fit on a single media.
Custom	Select this option to create your own rotation. You can select a rotation similar to the desired rotation prior to selecting the custom rotation type and the values from the previously selected rotation will remain as a starting place. The Calendar view is very helpful when creating custom rotations.

The Backup Export Tool provides a variety of media rotation types to select from, or you can define your own media rotation.

The following table compares the historical backups and full data recovery capabilities of each of the rotation types provided in the Backup Export Tool.

Table 8. Rotation Types Compared.

Rotation Type	# of Sets	Yearly Sets	Monthly Sets	Weekly Sets	Daily Sets
Simple	4		1 full	1 full	2 full
Simple	6		2 full	1 full	3 full
Simple	10		3 full	3 full	4 incremental
Simple	11		3 full	4 full	4 incremental
Simple	12		4 full	4 full	4 incremental
Daily Append	N (def. 4)			N full	4 incremental appends

Rotation Type	# of Sets	Yearly Sets	Monthly Sets	Weekly Sets	Daily Sets
GFS	20	2 full	6 full	6 full	6 incremental
GFS	25	2 full	7 full	8 full	8 incremental
GFS	30	2 full	8 full	8 fill	12 incremental

Schedule Settings

The **Schedule Settings** box contains several settings that control when jobs are run and how the jobs use media.

Schedule Type

The **Schedule Type** setting is the first step in choosing when the job is to run. Once scheduled, the Backup Export Tool service ensures the job is started. If one or more job runs are missed because the service is not running at the scheduled time, the service determines the backup mode with the largest interval setting (Daily, Weekly, Monthly, Yearly) that was missed, and runs it.

Table 9. Schedule Type.

Type	Description
Not scheduled	The job is run manually by the user when desired.
Run on selected days	The job runs only on a selected day (or days) at a specified time. When this option is selected an additional setting, **Scheduled Dates**, appears.
Run repeatedly	The job runs on a regular interval. Use this setting to set up a job with media rotation. When this option is selected an additional set of options, **Interval Settings**, appear.

Start Time

This setting is only visible for jobs that are to run on a schedule. It specifies the time of day that the job should start. For jobs that are scheduled to run more than once, all runs happen at the same time of day.

Rotation Type and Sets

This setting is only available when the job is scheduled to run repeatedly. The **Rotation type** and **Sets** controls allow you to specify a set of preconfigured rotations. The Custom Rotation type is a special case. It unlocks the user interface to allow the user to configure his own rotation.

Type of Fixed Rotation

This setting is only available when creating a custom rotation.

Scheduled Dates

This setting is only visible when the schedule type is set to run on selected days. It consists of a list of selected days to run the job. To add days to or remove days from the schedule, click **Calendar** to open the schedule calendar. To schedule the job to run on a day, right-click on the day in the calendar, and then click **Daily**. To unschedule a day, right-click on it, and then click **None**.

Interval Settings

This setting is only visible when the job is scheduled to be run repeatedly. It contains controls for specifying which types of jobs (full, incremental, or differential) are to be run on which intervals and the number of media sets that are to be used. Click **Calendar** to view of the schedule. The calendar displays when daily, weekly, monthly and yearly backups are to run. Clicking a day displays a message along the bottom of the dialog explaining the type of job that is to be run, the name of the media that is to be created, and whether the media is to be appended to or overwritten. To override the schedule on an individual day, right-click on the day, and then select the new backup type or deselect the day to stop the backup on that day.

> It is a good idea to deselect holidays from you schedule if you do not have a tape library or if no one will be available to put the correct media into the device.

Mode Settings

The **Mode** box contains several settings that control:

- Type of backup
- How automatic verify is performed
- How to treat used media
- What to do when a file does not fit on the current media.

Many of these settings are set automatically when a schedule rotation is in effect. When a rotation controls these settings, they are disabled in the Administrator.

Backup Mode

The Backup Export Tool supports the backup modes listed in the following table. For scheduled automatic rotation jobs, the Backup Export Tool uses the backup mode for each backup set as indicated on the **Schedule** page; for unscheduled or manual jobs, the Backup Export Tool uses the settings set by the user.

Table 10. Backup Mode.

Setting	Description
Full	This setting instructs the Backup Export Tool to back up all selected files.
Differential	This setting instructs the Backup Export Tool to back up all selected files that have changed since the last full backup.
Incremental	This setting instructs the Backup Export Tool to back up all selected files that have changed since the last full, differential, or incremental backup.
Copy	This setting instructs the Backup Export Tool to back up all selected files, but it has no effect on any future scheduled job. Use this option when you wish to make a record of files or systems at a particular time, but do not wish to disrupt the normal backup schedule.

Incremental jobs are the shortest and smallest jobs to run, but they present some issues related to full data recovery. The difference between an incremental and a differential backup is important: incremental backup jobs back up only files that have changed since the last full, differential, or incremental backup, while differential backup jobs back up all files changed since the last full backup. If incremental backup media sets are overwritten or recycled before another full backup is performed, this can create a gap in available data if you need to recover files from the overwritten media.

Exclusive use of incremental backup jobs to ensure full data recovery after a disaster is not recommended, unless you are using a schedule that retains one full backup and all subsequent incremental backups before overwriting any media. However, to ensure successful data recovery with incremental jobs, follow these guidelines:

- Have at least as many incremental media as there are days between full or differential backup jobs. For example, if you run full backup jobs every five days, have at least four incremental media; if you run full backup jobs every seven days, have at least six incremental media.
- Never recycle incremental media between differential or full backup jobs. If you run more than one incremental job in a row, be certain to not recycle any of the media used during this string of incremental jobs.

Auto Verify Mode

After the Backup Export Tool backs up a set of data, it can verify that the data was backed up correctly. The Backup Export Tool reads the files from the media and performs the selected verification type. If any discrepancies between the two files are found, the file is reported in the job log.

Table 11. Auto Verify Mode.

Verification Type	Description
Full Verify	This setting instructs the Backup Export Tool to compare every selected file stored on the media with the original file from the PC desktop or file or application server. If the file has changed since it was backed up, the full verify process reports that the file on the media does not match the file on disk. This does not mean that the backup was unsuccessful.
Quick Verify	This setting instructs the Backup Export Tool to be certain that every file backed up onto the media is in readable condition. It does not verify that the data matches the file, only that the data stored on the media can be read.
No Verify	This setting instructs the Backup Export Tool to skip the verification step. It is not recommended.

Verifying that data has been correctly written to the media is an essential part of a comprehensive backup program. Also, verifying the files ensures that the media and the media drive are working correctly.

Write Mode

For automatic rotation jobs, the Backup Export Tool overwrites all media. For other jobs, the Backup Export Tool uses the write mode settings set by the user. This mode determines whether the old data on the media is overwritten with new data or whether the new data is appended to the end of the old data. When media is overwritten, all of the data previously stored on it is lost. Appending data preserves the old data.

Table 12. Write Mode.

Setting	Description
Append to all media	This setting instructs the Backup Export Tool to append all data to the end of the media. No data is overwritten. Select this setting for permanent storage.
Append to first media, overwrite others	Append to first media, overwrite others.
Overwrite all media	This setting instructs the Backup Export Tool to overwrite all media. All data on media that is overwritten is lost. Use this option for media that are going to be recycled.

Split File

The Split File mode determines how the Backup Export Tool handles a file if the file is too large to fit on the current media. Select this option to instruct the Backup Export Tool to split a file across two media if it will not fit on the current backup media. If this option is not selected then files that do not fit on the media are restarted on the next media.

If you use the split file option, files that span two media require both media for restore. If one is lost then the file cannot be recovered. Files protected with split file mode cannot be restored during Disaster Recovery. They must be restored after the DR process has completed.

Media Settings

Select the folder where a job can look for existing media to reuse. Note that the default folder is the current Job folder. To use media from another folder, click **Add** to open a catalog browser and navigate to the desired folder.

Auto Format Mode

Before data can be written to media, the media must be formatted. When media is formatted, any data on it is lost and all record of the media is removed from the catalog.

Table 13. Auto Format Modes.

Mode	Description
No auto format	Instructs the Backup Export Tool to send an alert to the alert window if it encounters media that needs to be formatted (either blank or unrecognized media). While waiting for a user reply, the Backup Export Tool scans the network for devices with the media it was expecting.
Auto format blank media only	Instructs the Backup Export Tool to automatically format all new or blank media. However, if the Backup Export Tool encounters unrecognized media, it sends an alert to the alert window and then scans the network for the media it was expecting. This setting can help prevent data from being accidentally destroyed by formatting, while not needlessly querying the user before formatting a blank media.
Auto format all media	Instructs the Backup Export Tool to automatically format all of the media inserted into the tape drive which require formatting. With this setting selected, the Backup Export Tool automatically formats all new or blank media and all unrecognized media.

New Media Location

Specifies the folder in which the Backup Export Tool stores any new media created while the job is run. By default, the Backup Export Tool stores media under the backup job to ensure the media is not used by another backup job. To change the default, click **Browse** and select the folder from the **Browse** dialog box.

When the Backup Export Tool runs any scheduled automatic rotation job, it automatically creates

media folders for the job. The folders are organized by the name of the job and the various rotation sets in that job.

Move Media to New Media Location on Overwrite

Setting this check box moves media from the Media to be used folder to the New media location folder when it is used.

> If this option is turned off, it is possible for a job to exhaust its set of available media and stop running.

Rename Media to New Media

Selecting this check box renames any existing media that is overwritten to the name that would have been used had the media been freshly formatted. When this check box is cleared, already formatted media retains the name that it was given when it was previously used by this job.

New Media Name

Enter the name that the Backup Export Tool gives to any new media it creates while running a job. For scheduled automatic rotation jobs, the Backup Export Tool automatically updates this setting to match the media's place in the rotation schedule and this setting has no effect.

For manual rotation and unscheduled jobs, the Backup Export Tool assigns the name in this field to any new media that it creates. It also assigns this name for automatic rotation jobs that are "forced" to run. If the job creates more than one media, the job uses this setting as a template to create a unique media name from this setting.

Running Jobs in Rotation

The info bar displays the **Current rotation set** and the **Next rotation set** in the **Rotation Details** section of the info bar. Before the job is run the first time, both fields have the same value. Once the job runs successfully, the **Current rotation set** field displays the media that has just been used and the **Next rotation set** field displays the media that is to be used next.

Initial Run

The initial run of a rotation job uses the largest schedule interval in the rotation. For example, suppose a job is configured to begin a GFS 20 rotation on Thursday, October 28th, 2010. Even though a Thursday in the middle of a month would normally be classified as a Daily backup, the first time the job is run, the Backup Export Tool performs a Yearly backup.

Missed Jobs

If, for some reason, a run of the job is missed, for example, because the domain server was offline at the scheduled run time, the scheduler determines the largest interval missed and runs it automatically a few minutes after the Backup Export Tool starts up again.

Failed Jobs

If a job fails, the Backup Export Tool does not automatically run it again. However, you can manually rerun the job by clicking **Run** in the command bar.

Pausing and Continuing a Schedule

You can stop a scheduled job from running for a period of time by clicking **Pause Schedule** in the command bar. To turn the scheduled job back on, click **Continue Schedule** in the command bar. As with initial and missed jobs, the scheduler starts again with the largest schedule interval that was skipped.

Forcing a Run

At times it may be desirable to start a job before its regularly scheduled time. To run the next scheduled interval immediately, click **Run next schedule** in the command bar. When its originally scheduled time arrives, the job is not run again. Forcing a job to run ahead of its next scheduled time does not affect the schedule of subsequent runs, which resume their normal schedule.

Managing Devices

The Backup Export Tool recognizes any installed device that is part of the Backup Export Tool management domain and displays them on the Devices view. You can use the Devices view to perform operations on any physical or virtual device.

There are several physical operations that can be performed on a selected device. Some of these operations affect the device itself, while others affect the current media in the device.

> Not all operations are available on all devices. For example, an optical device does not support the Rewind command. Check your hardware documentation to determine which of the following commands are supported by your device. Only supported commands appear on the **context** menu and the command bar.

Identify

Use this command to get the name of the media currently loaded in the device. The Backup Export Tool attempts to identify the tape or other media that is currently loaded in the device. If the Backup Export Tool cannot identify the media, it reads the media header, a process that may take up to several minutes. The name of the media appears on the log file for the media job and in the Media column of the device list.

Import

This command allows you to use data on media that was created in another Backup Export Tool management domain. To use media that was not created in the current catalog, you must import that media into the current catalog.

You might import media in one the following situations:

- To use media created by an earlier version of the Backup Export Tool.
- To use media created in a different the Backup Export Tool management domain.
- To use media accidentally deleted from the catalog.

When you select the Import command a property page opens and prompts you for the media password and the encryption passphrase. The media password is only applicable to media created with older version of the Backup Export Tool and can usually be left empty.

An encryption passphrase is only required for encrypted media. If the supplied passphrase is not correct, the job log presents you with the hint supplied at the time of the media's creation.

Format

Use this command to format media currently loaded in the selected device.

When you format new media, the Backup Export Tool opens the **Format Media** dialog box. Use this dialog box to name the media and select a media folder in which to store the media. The Backup Export Tool formats the media currently loaded in the device you select. If you select a library, select the storage slot that holds the media you want to use. When you format media, you can also set your choice of encryption levels. Any backup job that uses media pre formatted with encryption must specify the same encryption parameters.

> The Backup Export Tool is designed to manage your media for you. This command should only be used by knowledgeable users and only after determining that the built-in media management does not produce the desired results.

Erase

This command erases the media currently loaded in the selected device.

Table 14. Erase Commands.

Command	Description
Quick Erase	Erases the first block and then writes an end of data marker to that first block. The other blocks of the tape are not erased, but when that tape is read, the Backup Export Tool treats it as if it were blank because it encounters the end of data marker in the first block.
Secure Erase	Erases every block on the tape. This operation can be very time consuming, lasting several hours. However, it will physically erase every block on the tape. If you want to destroy sensitive data, use this command.

Some devices support both options; some support only one of the two erase options. Only options supported by the selected device will be available.

Retension Media

Occasionally when a tape is repeatedly fast-forwarded and rewound for only short distances, tension differences develop in the tape that cause the tape drive to falsely believe it has reached the end or beginning of the tape. You can use this command to fast-forward the tape to the end of the tape and then rewinds it to the beginning. This command can be useful in some circumstances. By retensioning the tape, you can sometimes make an otherwise unusable tape operational again.

> If you need to retension tapes regularly to use them, consider servicing your tape drive or replacing your tapes.

Eject

You can use this command to eject media from the selected device or eject the media magazines from the selected library. Some libraries do not support ejecting media magazines using this command.

Restore Catalog

The **Restore Catalog** command provides a quick method of restoring your current catalog–for example in case it has been corrupted. For example, you might use this command if the Backup Export Tool Domain Server has crashed. Use this command only when your current set of media is intact.

The **Restore Catalog** command differs significantly from the **Import Media** command in that it

replaces the current catalog with the last known good catalog on that media. **The Import Media** command, on the other hand, does not replace the current catalog; it only adds additional data to it.

The advantage of the **Restore Catalog** command is that it provides a quick and easy way to replace a lost or corrupted the Backup Export Tool catalog. You could use the **Import Media** command to restore a corrupted catalog, but this process requires importing all of your media rather than simply reading the media containing the catalog.

Make a regular backup of the Backup Export Tool catalog. It is automatically included in any full backup of the Backup Domain.

All information in the current Backup Export Tool catalog will be lost when you use the **Restore Catalog** command. This command does not append data to the current catalog; it replaces the current catalog with the last known good catalog on that media.

You will be prompted stop and restart the service. Use the Backup Export Tool Service Control Manager to start and stop the Backup Export Tool service.

Clean Device

The **Clean Device** command will run the backup device through a cleaning cycle.

This command is supported only by libraries. If a device in a library provides notification that it needs cleaning and the library has a cleaning cartridge available, a cleaning cycle will be performed automatically at the start of a backup job. If you are using a device that is not a library, you must manually clean the device at the manufacturer’s suggested intervals.

To clean a device in a library, highlight the device and select **Clean Device** from the **Command** bar. The Backup Export Tool checks to see if one of the slots holds a cleaning cartridge. If it does, the cleaning cycle will be performed in the background; if not, an error message is shown.

If the **Clean Device** command is missing, it is not available for your backup device. In this case, a cleaning cycle can often be performed by manually inserting a cleaning cartridge into the backup device.

Start, Stop, and Rescan

Sometimes you will need to restart a device that has, for some reason, failed to initialize properly. A device may have stopped for any number of reasons, such as a power failure or a connecting cable malfunction. Virtual devices on a network appear disabled if the network connection has failed.

When a device is not initialized, it appears with a yellow warning icon. Some devices may take some time to initialize, during which the warning icon continues to display. If a device shows the warning icon after it is initialized, press **F5** to refresh the device display.

If you do not see a device that you expect to see connected to a machine, select the **Device** folder under the machine and click the **Rescan for New Devices** command.

If there is some other problem with the device or the controller, the warning icon continues to display. You must identify and correct the problem yourself. Then you must restart both the Backup Export Tool and the Backup Export Tool service. When the Backup Export Tool restarts, it initializes the device driver again. Check the **Devices** view to see that the devices are now properly working and that they no longer display the warning icon. Any duplicate or old devices that are offline can be deleted from the **Catalog** view.

Device Properties

When you select a specific device in the **Devices** view and click **Properties**, you can view the device status, configure settings, and review diagnostic information.

Status

The **Status** page displays the current status information for the selected device. For example, it shows the current operation, if any, being performed on the device. It also shows the last time a write and read was done on the device.

> The Backup Export Tool tracks the contents of devices and libraries while it is running. However, there may be times when someone changes media in a device or a library when the Backup Export Tool is not running. The "Probably" qualification on element status indicates that the Backup Export Tool has restarted and is operating under its previous understanding of the current element status but that the understanding may be incorrect. When "Probably" appears before an element status, the element's actual status is determined the next time the element is used.

Table 15. Status Information.

Status	Description
Valid	The slot is known to hold media that is in the current catalog.

Status	Description
Probably Valid	The slot held valid media previously. The Backup Export Tool verifies that the media is valid before using it. When you exit and restart the Backup Export Tool, media marked Valid is reset to Probably Valid.
Invalid	The slot holds media that is definitely not in the current catalog.
Probably Invalid	The slot holds media that may not be in the current catalog. When you exit and restart the Backup Export Tool, media marked Invalid is reset to Probably Invalid.
Empty	The slot is either known to be empty or a user changed its status to Empty.
Probably Empty	The slot was empty previously. When you exit and restart the Backup Export Tool, slots marked Empty are reset to Probably Empty.
Unknown	The status of the slot is not known, usually because it has not been used yet.
Cleaning Tape	A user marked the slot as holding a cleaning cartridge. The number of remaining cleaning cycles also appears. The Backup Export Tool does not verify that a cleaning cartridge was, in fact, inserted into this slot.
Probably Cleaning Tape	The slot previously contained a cleaning tape. When you exit and restart the Backup Export Tool, slots marked Cleaning Tape are reset to Probably Cleaning Tape.
Reserved	The slot was disabled by a user. The Backup Export Tool ignores it during any job. You can only change the status of a reserved slot. The Backup Export Tool changes the status of all other slots during normal operations.

Configuration

You can set the size of the I/O buffer to be used for this device. Usually, you do not need to change the default. However, for some devices, you may be able to increase performance by adjusting the size of the I/O buffer.

Diagnostics

The **Diagnostics** page displays device diagnostic information including information about the driver, the inquiry information, device statistics, and buffer statistics. Often this information can assist in troubleshooting problems. The diagnostics can be saved to a file or emailed directly from the diagnostic screen.

Sharing Storage Devices on a SAN

Backup jobs automatically select devices to use based on their availability (whether or not they are in use). In a SAN environment, the Backup Export Tool automatically recognizes that a single backup

device attached to a SAN may be accessible from two or more servers, and treats the device as a single device.

All machines that need access to a SAN server must be included in the same Backup Export Tool management domain.

Working with Tape Libraries

Tape libraries automate tape media handling which, in conjunction with the Backup Export Tool backup schedules, allows hands-off backup operations. A tape library contains one or more tape drives, some number of storage slots for tape media, and, in some cases, import/export slots to add or remove media from the library.

The Backup Export Tool The Backup Export Tool Server Backup tape library support includes managing media using barcodes, using the on-board memory in some tape cartridges, such as Ultrium Memory in Cartridge (MIC), and user-configurable tape media load ports (mail slots).

Always manage your tape media from the Backup Export Tool interface. Your tape library may provide a front panel that allows you to carry out various media management tasks but if you use this for media operations the Backup Export Tool catalog does not have the up-to-date media location information. For this reason, front panel media operations require time-consuming inventory processes to update the catalog.

If your library supports multiple tape devices and you want to use a specific device, you must select that device to use it. If you select the library, the Backup Export Tool uses the first available device in the library.

Installation and Configuration

If the tape library is installed correctly, the Backup Export Tool automatically detects the tape library. When detected, the tape library is added as an available device to the Backup Export Tool catalog.

Once you have installed the Backup Export Tool, expand the **Devices** view to locate the tape library. Note how the components of the tape library are displayed so that you can see how many devices (tape drives), import-export Slots (mail slots), and storage slots are associated with the library.

- **Devices** – The tape drives in a tape library are viewed and managed in the same way as stand-

alone tape drives.
- **Storage Slots** – The Storage Slots folder displays the number of available slots. Each slot may contain blank (new) media, media containing the Backup Export Tool data, or media containing unknown (non-Backup Export Tool) data. The Backup Export Tool inventories the media in the slots and displays the information about the media and its status in the view. This allows you to view all kinds of media, not just the media used by the Backup Export Tool, but you cannot select non-Backup Export Tool media for a backup or restore job.

It can take a long time to inventory the tape media in a tape library, which is why the Backup Export Tool usually performs a "light inventory" rather than running an identify job on all the slots in a loader. See the *Inventory Process* section below for more information.

Additional media slot configuration is accessed via the Element Status dialog for that slot, which is accessed by a right click on the desired slot. For example, you can use this to disable slots (using the 'Reserve' option) and identify a cleaning cartridge.

- **Import/Export Slots** – Some library devices provide special import/export mail slots an operator uses to enter or eject media to or from the device without removing the whole media repository or magazine. Depending on the device, more than one import/export slot can be provided. In case of a single mail slot, media are inserted one by one, while in case of multiple mail slots, a particular number of slots can be used in one enter/eject operation.

Barcodes and Memory in Cartridge

If the tape library supports barcode and/or MIC, the details are added to the Backup Export Tool catalog. The barcode information is hidden by default; to display this detail, right-click anywhere in the column title row to see available column headings and click on **Media barcode** to make the barcode information visible in the slots view.

Barcode and MIC technologies are used to reduce the time spent organizing and managing media in a library or an autoloader. In these devices, each medium is identified with a unique barcode or, where MIC is used, a chip is embedded in the tape cartridge which holds a unique identifier as well as other information.

Barcodes and MIC enable the Backup Export Tool to significantly reduce media recognition, labeling and cleaning tape detection times.

- Scanning the barcode or MIC of the media is faster than reading the medium header, because the Backup Export Tool does not need to actually load the media into a drive.
- A barcode or MIC is a unique identifier for media in the Backup Export Tool catalog. You should not have duplicate barcodes in your environment.

Barcode Filters

The barcode filter allows users to control access to media by barcode. The user can specify ranges, wildcards, or explicit barcodes that either include or exclude media for use by the product. This property only applies to libraries. Stand alone devices are not restricted in any way by it.

The filter rules may be set for the whole domain and will be applied automatically to all tasks. Or, they may be set and applied at job level. Any filter rules applied at job level overwrite the default domain settings.

For more information on setting barcode filters, see the *Barcode Job Filters* section.

Initialization Process

The traditional loader inventory mechanism is accomplished by running an identify job on all the slots in a library. This complete inventory can take a very long time, so the Backup Export Tool uses a "light inventory" process, which is known as an initialization process. This initialization process consists of:

- Checking that the loader is ready for use. If the magazine door is open, this step will fail, and initialization will fail as a result.
- Querying the number of physical storage, import/export and device elements that the library contains. (These elements display in the Tape Library view.)
- Binding the loader to its physical devices. This ensures that the devices are associated with the library in the Backup Export Tool catalog.
- Updating the status for each element in the loader. Barcodes are read at this time, and are associated with each element regardless of status (i.e., both Invalid and Valid elements get a barcode shown in the loader status pane).

Initialization occurs when the library driver starts (at service startup or when the driver is manually started), when the user selects the Initialize command on the loader object or when the Backup Export Tool detects that a user has changed the state of the loader (either by opening the front door or by using the front panel).

During initialization, the library attempts to perform barcode based identification of media. If a match is found, the loader sets that element’s status to Probably Valid. This means that if a user is using barcodes with their tape library, they rarely need to run an identification job.

When the job loads the tape it makes sure that the tape is really what the catalog says it is and, if necessary, updates the catalog to indicate what is really there. If the tape is, in fact, not usable because of the supplied media rules, the tape is re-stowed and another media is tried.

An Identify job always physically mounts media, and reassociates media to barcodes. This provides a mechanism for users to update barcodes on their media, if necessary. It also handles the case where barcodes are added to media after they have been used without barcodes.

Tape Media Management

One benefit of using the Backup Export Tool with tape libraries is the ease with which you can schedule different backups for different days of the week/month/year. There are no specific media tasks that must be carried out before you run a backup job. As long as the library has valid media loaded in it, the Backup Export Tool automatically uses it.

Media is invalid if it has been used by another backup product, is dirty or has been corrupted, or simply has not been identified.

Similarly, if you are restoring data from media that is already within the Backup Export Tool catalog, there are no media management tasks. However, if you are restoring media from a different domain, you must first import it so that the Backup Export Tool can add the media to the database and associate all data objects on the tape with that media.

For a detailed description of all media management jobs, see the *Device Commands* section.

Barcode Job Filters

Many tape libraries support the use of barcodes to identify media. Each piece of physical media has a unique barcode that the tape library can read.

The **Barcode Filter** page allows you to define barcode filters for a job. The filter rules may be set for the whole domain and will be applied automatically to all jobs. Or, they may be set and applied at job level, using this page. Any filter rules applied at job level overwrite the default domain settings. All options will be grayed out initially. Deselecting **Inherit settings from domain** enables the editing buttons and allows you to create job-specific filters.

There are three ways to assign barcode filters:

- **Add an individual barcode** – This option allows you to specify an individual barcode for inclusion or exclusion. Up to eight characters may be specified in this filter; the first six relate to the volume identifier and the last two relate to the media identifier. Wildcards may be used to increase the number of barcodes selected by the filter.
- **Add a range of barcodes** – This filter allows you to specify a range of volume identifiers and

media identifiers to include. Any media without a barcode or outside of the specified range is excluded.
- **Add barcodes from media present in the library** – This filter displays a list of all libraries and their elements. Select the required barcodes from the list and click either **Exclude** or **Include**, as appropriate.

Schedule Restore and Verify Jobs

Restore Job Settings

To schedule a restore job to happen at a particular time, change the **Schedule Type** to **Run on specific day** and then set the start time and date. The service ensures that the restore happens at that time.

Verify Job Settings

Like the restore job, you can schedule a verify to happen at a particular time as well. Additionally, you can specify whether the job is a Full or a Quick verify. A full verify compares the contents of the backup media with the source files on disk. A quick verify only validates that the media can be read from end-to-end.

Advanced Restore Options

These options apply to all restore jobs regardless of the operating system.

Table 16. Advanced Restore Options.

Option	Restore
General options	
Eject media after use	If selected, the Backup Export Tool automatically ejects the media at the end of the job. This feature only works on devices that support software eject.
Auto Retention	If selected, the Backup Export Tool automatically re-tensions the media at the beginning of the job. This feature winds the tape cartridge end-to-end, applying equal tension to the entire media for maximum media life and data integrity. Your device must support auto re-tension to use this feature.

Restore files that are in use	If selected, the Backup Export Tool restores the backup copy of the open file. (On Windows platforms, you can access the restored file after you restart the computer.) If you select this option, the restored file will replace your open file. As a result, your current changes may be lost. Deselect this option to skip over all selected files that are in use. This is useful if the open files are more current than the backed up files.
Omit security information	If selected, any security information associated with the files and folders which were part of the backup is removed. The files and folders are restored, as if they were freshly created, inheriting permissions.
Windows options	
Reparse points	Select this option to restore the reparse point data. When this option is deselected, the Backup Export Tool restores the object as a file or folder rather than as a reparse point.
Mount Points	When selected, the Backup Export Tool includes the mount point information in the restore. If this option is not selected, the Backup Export Tool restores the object as a directory.
Volume restrictions	When enabled, volume quota information will be restored.
Finalize recovery of Microsoft SQL and Exchange Server databases	Select this option to process database transactions when the last incremental restore is complete.
Restore all registry keys / Restore hardware registry keys	Controls whether/how the Backup Export Tool restores the described objects. This setting only applies if you restore the Registry System State object.
Restore DFS/FRS shares as primary replica (authoritative restore)	Use this option to control how a DFS or FRS share is being restored. Only select it if you want an authoritative restore. See the Microsoft documentation for more information on authoritative restores.

Data filters, such as security information and directory attributes, cannot restore data that was not originally backed up to the media. For example, if you did not select **Volume restrictions** for the backup job, the Backup Export Tool cannot restore this information because it was never stored on the media.

Advanced Verify Options

Table 17 lists the advanced options available for Verify jobs.

Table 17. Advanced Verify Options.

Option	Description
General options	

Eject media after use	When selected, the Backup Export Tool automatically ejects the media at the end of the job. This feature only works on devices that support software eject.
Auto Retention	When selected, the Backup Export Tool automatically re-tensions the media at the beginning of the job. This feature winds the tape cartridge end-to-end, applying equal tension to the entire media for maximum media life and data integrity. Your device must support auto re-tension to use this feature.
Native data streams format	When selected, the Backup Export Tool compares the data in native format. When unselected, only the data portion of the file is verified. This must match the mode used during backup.
Windows options	
Enable snapshots	By default, the verify job creates a temporary snapshot before verifying the selected file. Deselect this to disable snapshots.
Reparse points	Select to verify the reparse point data. When deselected, the Backup Export Tool verifies the object as a file or folder rather than as a reparse point.
Mount Points	When selected, the Backup Export Tool includes the mount point information in the restore. If this option is not selected, the Backup Export Tool verifies the object as a directory.
Volume restrictions	When enabled, volume quota information is verified.

Backup Export Tool Advanced Options

The options in the following tables are provided for advanced users who need to customize their backup jobs for unique circumstances. Unless you have specific needs that require changes to the advanced options, leave the default values unchanged.

Table 18. Settings for All Platforms.

Option	Description
Eject media after use	When selected, the Backup Export Tool automatically ejects the media at the end of the backup job. This feature only works on devices that support software eject.
Auto Retention	When checked, the Backup Export Tool automatically re-tensions the media at the beginning of the backup job. This feature winds the tape cartridge end-to-end, applying equal tension to the entire media for maximum media life and data integrity. Your device must support auto re-tension to use this feature.

Create DR bootable media	Select this option to write disaster recovery (DR) system information to the backup media. This option is only useful when the backup media is bootable as in the case of OBDR tapes or optical media. However, leaving this option checked does not hurt the backup.
Update DR information on selected machine	Check this option to generate DR system information for the selected machines. The generated system information is saved on the Domain Server and can be used later to create DR media even after a failure of the original machine.
Native data streams format	Different operating systems transmit data across the network to the Backup Export Tool in different formats. If you plan to restore files to a different operating system than the one in which they were created, the data should be stored on media in a common data format, not in the native data streams format.

Table 19. Settings for Windows

Option	Description
Enable snapshots	By default, the backup job creates a temporary snapshot before backing up the selected file. Deselect this checkbox to disable snapshots. A snapshot freezes the volume data at a point in time. Any subsequent changes are not backed up until the next backup job. The temporary snapshots are deleted after the job has finished. If this option is off, files open during backup may not be backed up. Failure to back up open files are noted in the job logs. Snapshots are currently implemented only on Windows platforms. Snapshots are created using Microsoft Volume Shadow Copy Services (VSS) for those Windows editions that support VSS.
Reparse points	Check this option to back up the reparse point data. When this option is deselected, the Backup Export Tool backs up the object as if it were a normal file or directory.
Mount Points	When selected, the Backup Export Tool includes the mount point information in the backup. If this option is not selected, the Backup Export Tool treats the object as a directory.
Optimize backup order by size	If selected, the Backup Export Tool mixes backups of large and small files in an attempt to maintain consistent throughput to the backup devices.
Volume restrictions	When enabled, volume quota information is backed up.

Backup Export Tool Supported Devices

The Backup Export Tools is designed to support families of devices regardless of the specific device model deployed. The system supports removable USB disks up to 128 TB.

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
Certance	Sidewinder 50	6.1	N/A	N/A	AIT-1
Certance	Sidewinder 70	6.1	N/A	N/A	AIT-1
Compaq	AIT 50	6.3 sp3c	N/A	N/A	AIT-2
Compaq	AIT 35	6.3 sp3c	N/A	N/A	AIT-1
Compaq	AIT 35 IDE	6.3 sp3c	N/A	N/A	AIT-1 IDE
Compaq	AIT 100	6.3 sp3c	N/A	N/A	AIT-3
Ecrix	VXA-1	6.2 sp2a	N/A	N/A	
Exabyte	EXB-8500	6	N/A	N/A	
Exabyte	VXA-320	8.1 sp1a	N/A	N/A	Windows, Linux only
Exabyte	Mammoth	6	N/A	N/A	EXB-8900
Exabyte	EXB-8205	6	N/A	N/A	1/2 high version of 8500C
Exabyte	VXA-172	8.1 sp2a	N/A	N/A	Windows, Linux only
Exabyte	Mammoth2	6.2 sp1b	N/A	N/A	
Exabyte	EXB-8700	6	N/A	N/A	Identifies self as 8505
Exabyte	VXA-2	6.3 sp3b	N/A	N/A	SCSI, IDE
Exabyte	EXB-8505	6	N/A	N/A	1/2 high version of 8500C
Exabyte	EXB-8500C	6	N/A	N/A	8500 w/compression
Exabyte	EXB-8200C	6	N/A	N/A	8200 w/compression
Exabyte	EXB-8200	6	N/A	N/A	
Exabyte	VXA-1	7.0 sp5b	N/A	N/A	
NEC	ND-6500A	8.1 sp1d	N/A	N/A	Windows/Linux only. Disaster Recovery NOT supported.
Sony	SDX-400C	6.2 sp3f	N/A	N/A	AIT-1
Sony	SDX-700C	6.3 sp2b	N/A	N/A	AIT-3
Sony	SDX-450V	7.0 sp7b	N/A	N/A	AIT-1 Turbo
Sony	SDX-250V	7.0 sp7b	N/A	N/A	AIT-E Turbo
Sony	SDX-560V	7.0 sp7b	N/A	N/A	AIT-2 Turbo, IDE
Sony	SDX-520V	7.0 sp5b	N/A	N/A	AIT-2, IDE
Sony	SDX-900V	7.0 sp7c	N/A	N/A	AIT-4
Sony	SDX-460V	8.1 sp2a	N/A	N/A	AIT-1, USB, AITe100T-UL, Windows only
Sony	SDX-700V	7.0 sp5b	N/A	N/A	AIT-3
Sony	SDX-260V	7.0 sp7b	N/A	N/A	AIT-E Turbo, IDE
Sony	SDX-800V	8.1 sp1c	N/A	N/A	
Sony	SDX-870V	8.5 sp0	N/A	N/A	AIT-3Ex, SATA

Sony	LIB-81/A4	7.0 sp7c	1	8	AIT-4
Sony	SDX-570V	8.1	N/A	N/A	
Sony	SDX-470V	8.1	N/A	N/A	
Sony	SDX-460V, IDE	7.0 sp7b	N/A	N/A	AIT-1 Turbo
Sony	SDX-560V	8.1 sp2a	N/A	N/A	AIT-2, USB, AITe200T-UL, Windows only
Sony	SDX-520C	6.3 sp3c	N/A	N/A	AIT-2, IDE
Sony	SDX-300C	6.1	N/A	N/A	AIT-1
Sony	SDX-500V	7.0 sp2c	N/A	N/A	AIT-2
Sony	SDX-420V	7.0 sp5b	N/A	N/A	AIT-1, IDE
Sony	SDX-500C	6.2 sp1a	N/A	N/A	AIT-2
Sony	SDX-400V	7.0 sp2c	N/A	N/A	AIT-1
Sony	SDX-1100	8.1 sp3a	N/A	N/A	AIT-5 SCSI
Sony	SDX-420C	6.3 sp3c	N/A	N/A	AIT-1, IDE
Sony	SDX-550V	7.0 sp7b	N/A	N/A	AIT-2 Turbo
Tandberg	VXA-320	8.1 sp1	N/A	N/A	Windows and Linux only

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
OnStream	ADR50	6.2	N/A	N/A	50, 50e
OnStream	ADR2.120	6.3 sp2a	N/A	N/A	Si,Se
OnStream	ADR2.120	6.3 sp3b	N/A	N/A	ide
OnStream	ADR2.60	6.3 sp2a	N/A	N/A	usb
OnStream	ADR30	6.2	N/A	N/A	Not Di30
OnStream	ADR2.60	6.3 sp1a	N/A	N/A	Si,Se,ide

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
IBM	TS2900 LTO4 HH SAS	9.0	1	9	
IBM	TS2900 LTO5 HH SAS	9.0	1	9	
IBM	TS2900 LTO6 HH SAS	10.0.01	1	9	

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
HL-DT-ST	GCE-8487B	8.1 sp3a	N/A	N/A	CD-RW
HL-DT-ST	GCC-4482B	8.1 sp1d	N/A	N/A	CD-RW/DVD-ROM
HL-DT-ST	GSA-4163B	8.1 sp1d	N/A	N/A	DVD+/-RW
HL-DT-ST	GWA-4166B	8.1 sp1d	N/A	N/A	DVD+/-RW
Lacie	ND-2500A	8.1 sp1d	N/A	N/A	Windows/Linux only. Disaster Recovery NOT supported.
LG	GCE-8483B	8.1 sp1d	N/A	N/A	Windows/Linux only. Disaster Recovery NOT supported.

Lite-On	SOHC-4836V	8.1 sp1d	N/A	N/A	CD-RW/DVD-ROM
Lite-On	SOHC-4836K	8.1 sp1d	N/A	N/A	CD-RW/DVD-ROM
Lite-On	SOHC-4836B	8.1 sp1d	N/A	N/A	CD-RW/DVD-ROM
Lite-On	SOHW-1673S	8.1 sp1d	N/A	N/A	DVD+/-RW
Lite-On	SOHR-4839S	8.1 sp1d	N/A	N/A	CD-RW
NEC	ND-3540A	8.1 sp1d	N/A	N/A	DVD+/-RW
Plextor	504UF	8.1 sp1d	N/A	N/A	
Plextor	712UF	8.1 sp1d	N/A	N/A	Windows/Linux only. Disaster Recovery NOT supported.
Plextor	PX-712A	8.1 sp1d	N/A	N/A	DVD+/-RW
Plextor	PX-W5224A	8.1 sp1d	N/A	N/A	CD-RW/DVD-ROM
Samsung	SW-252S	8.1 sp1d	N/A	N/A	IDE, USB.
Sony	CRX216E	8.1 sp1d	N/A	N/A	CD-RW/DVD-ROM
Sony	PCGA-DDRW2	8.1 sp1d	N/A	N/A	DVD+/-RW
Teac	DW-224E	8.1 sp3a	N/A	N/A	CD-RW/DVD-ROM
Toshiba	TS-H492C	8.1 sp1d	N/A	N/A	CD-RW/DVD-ROM

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
Hewlett Packard Enterprise	D2D2500 Backup System (iSCSI)	8.7	N/A	N/A	
Hewlett Packard Enterprise	D2D4000 Backup System (iSCSI)	8.7	N/A	N/A	
Hewlett Packard Enterprise	D2D4112 Backup System	8.7	N/A	N/A	FC, iSCSI

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
AIWA	GD-24000	6.2 sp1b	N/A	N/A	DDS-3
AIWA	HP NCE	6.1	N/A	N/A	DDS-2, GD-8000
AIWA	GD-8000	6	N/A	N/A	DDS-2
Archive	4586XX	6	N/A	N/A	
Archive	4320XX (Python)	6	N/A	N/A	
Archive	Python	6	N/A	N/A	
Archive	4326XX (Python)	6	N/A	N/A	
Archive	4324XX (Python)	6	N/A	N/A	
Certance	STD 2400N	6.1	N/A	N/A	DDS-1 w/compression
Certance	STD 240LW	6.1 sp2d	N/A	N/A	DDS-4 Scorpion 40
Certance	STD 28000N	6.1	N/A	N/A	DDS-2
Certance	STD 224000N	6.1	N/A	N/A	DDS-3

Certance	STD 2200N	6.1	N/A	N/A	DDS-1
Certance	DAT 72	7.0	N/A	N/A	
Compaq	TSL-9000	6.2 sp1a	N/A	N/A	8 slot DDS-3 integrated loader
Compaq	TSL-10000	6.2 sp4b	N/A	N/A	8 slot DDS-4 integrated loader
Compaq	SDT-7000	6.2	N/A	N/A	DDS-2
Compaq	SDT-10000	6.2	N/A	N/A	DDS-4
Compaq	SDT-9000	6.2	N/A	N/A	DDS-3
DEC	TLZ07	6.1 sp2d	N/A	N/A	
Dell	PV-100T DDS4	6.3 sp2b	N/A	N/A	
Dell	PV-114T DAT72	7.0 sp7d	N/A	N/A	
Dell	PV-100T Dat72	7.0 sp7c	N/A	N/A	
Exabyte	4200C	6	N/A	N/A	DDS-1 w/compression
Exabyte	4200	6	N/A	N/A	DDS-1
Hewlett Packard Enterprise	DAT160 SAS	8.5 sp.1	N/A	N/A	DDS4,DAT72,DAT160
Hewlett Packard Enterprise	DAT160 SCSI	8.5 sp.1	N/A	N/A	DDS-4, DAT72, DAT160
Hewlett Packard Enterprise	DAT 320	8.7	1	N/A	USB, SAS
Hewlett Packard Enterprise	DAT160 USB	8.5 sp.1	N/A	N/A	DDS4, DAT72, DAT160
Indigita	iDT-2500	6	N/A	N/A	4mm (Not DAT format though)
Indigita	iDT-2700	6	N/A	N/A	4mm (Not DAT format though)
Quantum	DAT160 SAS	8.5 sp.1	N/A	N/A	DDS4,DAT72,DAT160
Quantum	DAT 72	8.1 sp1c	N/A	N/A	SATA, SCSI
Quantum	DAT160 USB	8.5 sp.1	N/A	N/A	DDS4, DAT 72, DAT 160
Quantum	DAT160 SCSI	8.5 sp.1	N/A	N/A	DDS4, DAT 72, DAT 160
Sony	SDT-7000	6	N/A	N/A	DDS-2 SE i/f
Sony	SDT-2000	6	N/A	N/A	DDS-1, discontinued
Sony	TSL-11000	6.2 sp3a	N/A	N/A	DDS-4 in integrated loader with SE/LVD i/f
Sony	SDT-11000	6.2	N/A	N/A	DDS-4 with SE/LVD SCSI i/f
Sony	TSL-10000	6.2 sp3a	N/A	N/A	DDS-4 in integrated loader with SE i/f
Sony	SDT-4000	6	N/A	N/A	DDS-1, discontinued
Sony	SDT-10000	6.1 sp2d	N/A	N/A	DDS-4 SE i/f
Sony	SDT-5000	6	N/A	N/A	DDS-1, discontinued
Sony	TSL-9000	6.1	N/A	N/A	DDS-3 in integrated loader

Sony	SDT-5200	6	N/A	N/A	DDS-1, discontinued
Sony	TSL-7000	6.1	N/A	N/A	DDS-2 in integrated loader
Sony	SDT-9000	6	N/A	N/A	DDS-2 SE i/f
Tandberg	DAT 72	8.1	N/A	N/A	SCSI and USB
Tandberg	DAT 160	8.5 sp1	N/A	N/A	SCSI and USB
Tandberg	DAT 320	8.7	N/A	N/A	SAS and USB
WangDAT	2600	6	N/A	N/A	DDS/DC (obsolete)
WangDAT	1300	6	N/A	N/A	DDS (obsolete)
WangDAT	3100	6	N/A	N/A	DDS-1
WangDAT	3300DX	6	N/A	N/A	DDS-2
WangDAT	3800DX	6	N/A	N/A	id as 3400 but added in case
WangDAT	3900DX	6	N/A	N/A	Never happened
WangDAT	3200	6	N/A	N/A	DDS-1 w/compression
WangDAT	3400DX	6	N/A	N/A	DDS-2 w/compression

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
Cipher	L860s	6	N/A	N/A	7 slot integrated loader w/6 GB DLT
Cipher	T860s	6	N/A	N/A	6 GB DLT
Cipher	L826s	6	N/A	N/A	7 slot integrated loader w/2.6 GB DLT
Cipher	T826s	6	N/A	N/A	2.6 GB DLT
Compaq	DLT 4000	6.2 sp1a	N/A	N/A	
Compaq	VS80	6.3 sp3c	N/A	N/A	
Compaq	100GB SDLT	6.3 sp3c	N/A	N/A	SuperDLT1
Compaq	DLT 8000	6.3 sp3c	N/A	N/A	
Compaq	160GB SDLT	6.3 sp3c	N/A	N/A	SDLT320
Compaq	DLT 7000	6.2 sp1a	N/A	N/A	
Compaq	DLT 8000	6.2 sp1a	N/A	N/A	
DEC	DLT 4500	6	N/A	N/A	5 slot loader w/DLT 4000
DEC	DLT 2000	6	N/A	N/A	
DEC	DLT 2500	6	N/A	N/A	5 slot loader w/DLT 2000
DEC	TZ87	6.2	N/A	N/A	DLT 7000
DEC	TZ89	7.0 sp2a	N/A	N/A	DLT 7000
DEC	DLT 7000	6.1	N/A	N/A	indentifies as TZ87

DEC	DLT 4700	6	N/A	N/A	7 slot loader w/DLT 4000
DEC	DLT 2700	6	N/A	N/A	7 slot loader w/DLT 2000
DEC	DLT 4000	6	N/A	N/A	
Dell	PV-114T SDLT320	7.0 sp7d	N/A	N/A	
Dell	PV-114T DLT VS160	7.0 sp7d	N/A	N/A	
Dell	PV-110T SDLT320	6.3 sp2b	N/A	N/A	
Dell	PV-110T DLT VS160	6.3 sp3b	N/A	N/A	
Dell	PV-110T DLT VS80	6.3 sp2b	N/A	N/A	
Quantum	DLT 4500	6	N/A	N/A	DLT 4000, 5 slot integrated loader
Quantum	Super DLT 220	6.2 sp3c	N/A	N/A	
Quantum	DLT 2500	6	N/A	N/A	5 slot integrated loader
Quantum	DLT-S4	8.1 sp2a	N/A	N/A	
Quantum	DLT 7000	6.1	N/A	N/A	
Quantum	SDLT600	7.0 sp5b	N/A	N/A	
Quantum	DLT 4700	6	N/A	N/A	7 slot integrated loader
Quantum	DLT 4000	6	N/A	N/A	
Quantum	DLT-V4	7.0 sp7c	N/A	N/A	SCSI (TapeWare 7 requires this patch, SATA (8.1 sp1c))
Quantum	DLT 2000	6	N/A	N/A	
Quantum	VS160	6.3 sp3d	N/A	N/A	
Quantum	DLT 8000	6.1 sp2d	N/A	N/A	
Quantum	DLT 2700	6	N/A	N/A	7 slot integrated loader
Quantum	Super DLT 320	6.3 sp3a	N/A	N/A	
Quantum/Benchmark	VS80	6.2 sp4b	N/A	N/A	
Quantum/Benchmark	Blade 640	6.3 sp3a	N/A	N/A	VS80 Autoloader
Quantum/Benchmark	VS160	6.3 sp3b	N/A	N/A	Benchmark Version
Quantum/Benchmark	DLT1	6.2 sp3e	N/A	N/A	BTS100, BNCHMRK DLT1, or BNCHMARK DLT1
StorageTek	9840	6.2 sp4b	N/A	N/A	
Tandberg	SDLT220	7.0 sp2c	N/A	N/A	
Tandberg	DLT-V4	8.1	N/A	N/A	SCSI, SATA (8.1 sp1c)
Tandberg	SDLT600	7.0 sp5b	N/A	N/A	
Tandberg	VS160	6.3 sp3d	N/A	N/A	

Tandberg	DLT 4000	6.2 sp1b	N/A	N/A	
Tandberg	DLT 8000	6.2 sp1b	N/A	N/A	
Tandberg	DLT 7000	6.2 sp1b	N/A	N/A	
Tandberg	SDLT320	7.0 sp2c	N/A	N/A	

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
Acer	Altos LTO-2 Autoloader	8.1 sp1c	1	8	
Archive	Python DAT	6.0	1	4-12	
BDT	ThinStor	6.3 sp3a	1	8	DLT VS, DLT, SDLT, LTO
BDT	ThinStorPlus	8.1 sp1c	1	8	
Certance	DAT432 Autoloader	7.0 sp3a	1	6	Seagate branded
Certance	SuperLoader 3	8.1 sp2b	1	8	
Certance	DAT 240	6.2 sp2a	1	6	240 GB
Certance	LDR	6.1 sp2c	1	4	AIT-1
Certance	LTO3 Autoloader	7.0 sp5c	1	8	CLL6400
Certance	LTO2 Autoloader	7.0 sp5b	1	8	CLL3200
Certance	DAT 96	6.2 sp3e	1	6	96 GB
Certance	LTO Autoloader	7.0 sp2a	1	8	CLL1600
Cipher	TZ Media Changer	6.0	1	7	DLT
Compaq	TSL-A300C	6.3 sp3c	1	4	AIT-1
Compaq	TSL-7000	6.3 sp3c	1	8	DDS-2
Compaq	LIB-81	6.3 sp3c	1	8	AIT-1, AIT-2, AIT-3
Compaq	TSL-11000	6.3 sp3c	1	8	DDS-4
Compaq	TSL-10000	6.1 sp4b	1	8	DDS-4
Compaq	TSL-A500C	6.3 sp3c	1	4	AIT-2
Compaq	TSL-9000	6.1 sp1a	1	8	DDS-3
Compaq	TSL-A400C	6.3 sp3c	1	4	AIT-1
DEC	DLT 2700	6.0	1	7	
DEC	TZ Media Changer	6.1	1	7	DLT
DEC	TL800	7.0 sp2a	1-2	10	DLT
DEC	DLT 4500	6.0	1	5	
DEC	DLT 2500	6.0	1	5	
DEC	DLT 4700	6.0	1	7	

Dell	PV-124T	7.0 sp5c	1	16	VS160, LTO-2, Must apply this patch (TW7 only): zip, LTO3
Dell	TL2000	8.1 sp3a	2	24	8.5 sp2 needed for LTO4, 8.8.03 needed for LTO5
Dell	PV-122T	6.3 sp2b	1	8	VS80, SDLT, LTO , LTO-2
Dell	PV-120T	6.3 sp2b	1	8	DDS4
Dell	PV-136T	7.0 sp2a	1-6	60-72	SDLT, LTO, LTO-2 , LTO-3
Dell	PV-132T	7.0 sp2a	1-2	21-24	SDLT, LTO, LTO-2 , LTO-3
Dell	PowerVault ML6000	8.1 sp1b	1-18	41-409	8.5 sp2 needed for LTO4, 8.8.03 needed for LTO5
Dell	TL4000	8.1 sp3a	4	48	8.5 sp2 needed for LTO4, 8.8.03 needed for LTO5
Exabyte	18D	6.1 sp2c	1	18	DLT
Exabyte	110L	6.1 sp4b	1	10	LTO
Exabyte	Magnum 1x7	7.0 sp7d	1	7	LTO-2, LTO-3
Exabyte	210	6.0	1	10+1	8mm
Exabyte	X200	-	2-10	40-200	Mammoth
Exabyte	215M	6.1 sp4b	1-2	15	Mammoth
Exabyte	EXB-10e	6.0	1	10	8mm
Exabyte	220	6.1 sp2c	2	20	8mm
Exabyte	690D	6.2 sp4b	2-6	30-90	DLT
Exabyte	PacketLoader 1x10 1U (VXA-2)	7.0 sp4c	1	10	
Exabyte	PacketLoader 1x10 1U (VXA-320)	8.1 sp1a	1	10	
Exabyte	X80	-	2-8	40-80	Mammoth
Exabyte	EXB-10i	6.0	1	10	8mm
Exabyte	230D	6.2	1-2	30	DLT
Exabyte	440/480	6.1 sp2c	4	40/80	8mm
Exabyte	PacketLoader 1x7	6.3 sp3b	1	7	VXA-2, identifies as EZ17
Exabyte	EXB-10h	6.0	1	10	8mm

Exabyte	StorageLoader	8.1 sp0	1	8	LTO-2
Exabyte	430	6.1 sp4b	1-4	30	Mammoth2, VXA-2, 430M
Exabyte	EXB-218	6.1 sp2c	1-2	18	DDS-2
Exabyte	221L	6.1 sp4b	1-2	21	LTO
Exabyte	EZ17	6.1 sp2c	1	7	8mm, VXA-1, VXA-2
Exabyte	PacketLoader 1x10 2U	7.0 sp7c	1	10	VXA-2
Gateway	Gateway E-826R SuperLoader3	8.1 sp2b	1	8	
Gateway	823		N/A	8	
Hewlett Packard Enterprise	1/8 G2 Tape Autoloader	8.1 sp3a	1	8	8.5 sp2 needed for LTO4, 8.8.03 needed for LTO5, 10.0.00 needed for LTO6, 10.5.00 for LTO7
Hewlett Packard Enterprise	MSL2024 Tape Library	8.1 sp2a	2	24	8.5 sp2 needed for LTO4, 8.8.03 needed for LTO5, 10.0.00 needed for LTO6, 10.5.00 for LTO7
Hewlett Packard Enterprise	MSL4048 Tape Library	8.1 sp2a	4	48	8.5 sp2 needed for LTO4, 8.8.03 needed for LTO5, 10.0.00 needed for LTO6, 10.5.00 for LTO7
Hewlett Packard Enterprise	MSL8048 Tape Library	8.7	4	48	8.8.03 needed for LTO5, 10.0.00 needed for LTO6, 10.5.00 for LTO7
Hewlett Packard Enterprise	MSL8096 Tape Library	8.7	4	96	8.8.03 needed for LTO5, 10.0.00 needed for LTO6, 10.5.00 for LTO7
Hewlett Packard Enterprise	MSL G3 Library Extender Kit	8.7	N/A	N/A	
Hewlett Packard Enterprise	MSL6840 Tape Library	10.5	42	560	10.5.00 for LTO5, LTO6, LTO7
Hewlett Packard Enterprise	ESL G3 Tape Library	10.5	192	12006	10.5.00 for LTO5, LTO6, LTO7

IBM	TS3310 Tape Library	8.7	2	35	If encryption is to be used, the library needs to be set to use the “application” controlled hardware encryption mode
IBM	TS2900 LTO-3	8.7	1	9	SAS
IBM	TS2900 LTO-4	8.7	1	9	SAS
IBM	Magstar MP 3570	6.2 sp4c	1-2	10	
IBM	ULT 3581-TA	6.1 sp4b	1	7	LTO
IBM	ULT 3583-TL	6.1 sp4b	1-6	18-72	LTO
IBM	TS3100	8.5	2	24	LTO3, LTO4
IBM	Magstar 3590	6.2 sp4c	1	10	
IBM	TS3200	8.5 sp2	4	48	8.8.03 needed for LTO5
Iomega	REV 280	8.5	1	8	Windows Linux: (2.6 kernel distos only)
Iomega	REV Autoloader 1000	7.0 sp7b	1	10	Windows only.
MediaLogic ADL	SLA8	6.2	1-6	26-49	8mm
Overland	LoaderXpress (LXL)	6.3 sp3c	1	10	DLT, SuperDLT, LTO
Overland	PowerLoader (LXM)	6.3 sp3c	1-2	15-17	DLT, SuperDLT, LTO
Overland	LibraryXpress (LXB)	6.2	1-16	10-138	DLT
Overland	Library Pro	6.2 sp3f	1-18	19-171	AIT only support up to 16
Overland	Neo Series	6.3 sp3c	1-16	24-240	2000 only, DLT, SDLT, LTO
Qualstar (TLS Series)	TLS-6110	6.2sp4c	1	10	DLT
Qualstar (TLS Series)	TLS-2472	6.1sp2c	4	72	4mm
Qualstar (TLS Series)	TLS-2436	6.1sp2c	4	36	4mm
Qualstar (TLS Series)	TLS-2236	6.1sp2c	2	36	4mm
Qualstar (TLS Series)	TLS-24144	6.1sp2c	4	144	4mm
Qualstar (TLS Series)	TLS-6220	6.2sp4c	2	20	DLT
Qualstar (TLS Series)	TLS-4660	6.3sp1b	4	60	8mm, DLT
Qualstar (TLS Series)	TLS-4210	6.1sp2c	2	10	8mm

Qualstar (TLS Series)	TLS-46120	6.2sp4c	6	120	8mm
Qualstar (TLS Series)	TLS-6210	6.2sp4c	2	10	DLT
Qualstar (TLS Series)	TLS-4220	6.1sp2c	2	20	8mm
Qualstar (TLS Series)	TLS-4480	6.1sp2c	4	80	8mm
Qualstar (TLS Series)	TLS-4440	6.1sp2c	4	40	8mm
Qualstar (TLS Series)	TLS-4210A	6.1sp2c	2	10	8mm
Qualstar (TLS Series)	TLS-4420	6.1sp2c	4	20	8mm
Qualstar (TLS Series)	TLS-6430	6.2sp4c	4	30	DLT
Qualstar (TLS Series)	TLS-6460	6.2sp4c	4	60	DLT
Qualstar (TLS Series)	TLS-2218	6.1sp2c	2	18	4mm
Qualstar (TLS Series)	TLS-2218A	6.1sp2c	2	36	4mm
Quantum	DLT 4700	6.0	1	7	
Quantum	DLT 4500	6.0	1	5	
Quantum	DLT stor314	6.2 sp5b	1	7	
Quantum	ATL P2000	6.3 sp3c	10	100-198	DLT, LTO
Quantum	SuperLoader 3	8.8.03	1	16	LTO-5
Quantum	ATL P3000	6.3 sp3c	16	170-326	DLT, LTO
Quantum	SuperLoader 3	8.1 sp2b	1	16	DLT VS160, DLT-V4, SDLT 600, DLT-S4, LTO-2 HH, LTO-3, LTO-3 HH, LTO-4
Quantum	SuperLoader	7.0 sp2c	1	16	DLT1, SDLT, LTO
Quantum	Scalar i40	8.9	2	25-40	LTO-5
Quantum	Scalar i500	8.1 sp1b	1-18	41-409	8.5 sp2 needed for LTO4, 8.8.03 needed for LTO5
Quantum	ATL L500	6.1 sp2c	1-3	14	DLT
Quantum	PX500 Series	8.1 sp2a	1-24	32-440	SDLT600, Disaster Recovery is untested
Quantum	DLT 2500	6.0	1	5	
Quantum	DLT 2700	6.0	1	7	
Quantum	Powerstor L200	6.2 sp5b	1	7	
Quantum	Scalar i80	8.9	5	25-40	LTO-5
Quantum	Scalar 24	8.5 sp2	N/A	N/A	LTO-4 SCSI
Quantum	ATL P1000	6.1 sp2c	1-4	30	DLT
Quantum / ADIC	Scalar AIT 220	6.1 sp1b	2	20	

Quantum / ADIC	VLS 4mm	6	2	15	DDS-1, DDS-2
Quantum / ADIC	FastStor 22	6.2	2	22	DLT
Quantum / ADIC	Scalar 218	6.1	2	18	DLT
Quantum / ADIC	DAT AutoChanger	6	1	12	
Quantum / ADIC	Scalar 1000	6.3 sp3c	1-12	118-237	AIT, DLT, SDLT, LTO
Quantum / ADIC	FastStor	6.1	1	7	DLT, LTO
Quantum/Benchmark	Blade 640	6.3 sp3a	1	8	VS80
Sony	LIB-D81/AIT-2 Turbo	7.0 sp7b	1	8	SDX-550V
Sony	TSL-A300C	6.2 sp2a	1	4	AIT-1
Sony	TSL-A500C	6.2 sp2a	1	4	AIT-2
Sony	LIB-D81/A5	8.1 sp3a	1	8	AIT-5
Sony	TSL-7000	6.0	1	8	DDS-2
Sony	LIB-81	6.3 sp3a	1	8	AIT-1, AIT-2, AIT-3
Sony	LIB-81/A5	8.1 sp3a	1	8	AIT-5
Sony	LIB-162	7.0 sp2a	2	16	AIT-1, AIT-2, AIT-3
Sony	LIB-81/A3Ex	8.1 sp1c	1	8	SDX-800V
Sony	LIB-162/A4	7.0 sp7c	2	16	AIT-4
Sony	LIB-162/A3Ex	8.1 sp1c	2	8	SDX-800V
Sony	LIB-D81/A3Ex	8.1 sp1c	1	8	SDX-800V
Sony	TSL-10000	6.2 sp3a	1	8	DDS-4
Sony	LIB-D81	7.0 sp2a	1	8	AIT-1, AIT-2, AIT-3
Sony	TSL-A400C	6.2 sp4b	1	4	AIT-1
Sony	LIB-162/A5	8.1 sp3a	2	16	AIT-5
Sony	LIB-D81/A4	7.0 sp7c	1	8	AIT-4
Sony	TSL-11000	6.2 sp3a	1	8	DDS-4
Sony	TSL-9000	6.1	1	8	DDS-3
Spectra Logic	Gator	6.3 sp3a	1-32	30-645	20k or 64k, AIT-1, AIT-2, AIT-3
Spectra Logic	Bullfrog	6.3 sp3a	1-4	20-40	10k, AIT-2, AIT-3
Spectra Logic	215	6.1	1	15	Travan
StorageTek	L180	6.2 sp4c	1-10	84-174	DLT, SDLT, LTO
StorageTek	L20	6.2 sp4a	2	20	DLT, SDLT, LTO
StorageTek	9730	6.2 sp2a	1-4	30	DLT
StorageTek	9714	6.2	1-6	40-100	DLT
StorageTek	L40	6.2 sp4a	4	40	DLT, SDLT, LTO

Sun StorageTek	SL24	8.1 sp2a	2	24	8.5 sp2 needed for LTO4, 8.8.03 needed for LTO5
Sun StorageTek	SL48	8.1 sp2a	4	48	8.5 sp2 needed for LTO4, 8.8.03 needed for LTO5
Tandberg	StorageLoader	7.0 sp7c	1	8	LTO2 only
Tandberg	StorageLibrary T24	8.8.03	2	24	LTO-3, LTO-4, LTO-5
Tandberg	Storageloader 1x8	8.5 sp2	1	8	8.5 sp2 needed for LTO4, 8.8.03 needed for LTO5
Tandberg	StorageLibrary T48	8.8.03	4	48	LTO-3, LTO-4, LTO-5
Tandberg	SDLT Autoloader	7.0 sp5c	1	10	NEC inquiry string
Tandberg	TDS-1210	6.2	1-2	10	QIC
Tandberg	StorageLoader LTO3	8.1 sp3a	1	10	
Tandberg	TDS-1440	6.2	2-4	40	QIC
Tandberg	LTO Autoloader	7.0 sp5c	1	10	NEC inquiry string
Tandberg	SuperLoader	7.0 sp2c	1	16	DLT1, SDLT
Tandberg	StorageLoader VXA (VXA-172/320)	8.1 sp1a	1	10	VXA-172, VXA-320
Tandberg	StorageLoader	8.1 sp0	1	8	LTO1, LTO2
Tandberg	TDS-1420	6.2	1-2	20	QIC
Tandberg	StorageLoader VXA (VXA-2)	7.0 sp4c	1	10	VXA-2
Tandberg	SLR Autoloader	6.2 sp4a	1	8	QIC
WangDAT	LD8	6.2	1	8	DDS-3

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
Certance	Ultrium 3	7.0 sp5c	N/A	N/A	
Certance	Ultrium 2	7.0 sp5b	N/A	N/A	
Certance	Ultrium 2 HH	7.0 sp5c	N/A	N/A	
Certance	Ultrium	6.3 sp1b	N/A	N/A	Ultrium 1
Dell	PV-110T LTO-3	7.0 sp7c	N/A	N/A	LTO3
Dell	PV-114T LTO-3	7.0 sp7d	N/A	N/A	
Dell	PV-110T LTO-3-L	8.1 sp3a	N/A	N/A	LTO3 half-height
Dell	PV-114T LTO-2-L	7.0 sp7d	N/A	N/A	
Dell	PV-114T LTO-2	7.0 sp7d	N/A	N/A	

Dell	PV-110T LTO-2-L	8.1 sp0	N/A	N/A	
Dell	PV-110T LTO-2	6.3 sp3b	N/A	N/A	
Dell	PowerVault LTO4-120	8.1 sp3a	N/A	N/A	SAS (HW encryption in 8.5 sp0 only)
Dell	PowerVault LTO3-060	8.1 sp3a	N/A	N/A	
Dell	PV-110T LTO	6.3 sp2b	N/A	N/A	LTO1
Exabyte	Magnum LTO-2	7.0 sp7c	N/A	N/A	
Hewlett Packard Enterprise	Ultrium 3280 Tape Drive	8.8.03	N/A	N/A	LTO5
Hewlett-Packard	Ultrium 960	7.0 sp7a	N/A	N/A	Ultrium 3
Hewlett-Packard	Ultrium 920	8.1 sp2a	N/A	N/A	SCSI, SAS (8.1 sp3a)
Hewlett Packard Enterprise	Ultrium 1840 Tape Drive	8.5 sp2	1	N/A	LTO4
Hewlett Packard Enterprise	Ultrium 1760 Tape Drive	8.5 sp2	1	N/A	LTO4
Hewlett Packard Enterprise	Ultrium 3000 Tape Drive	8.8.03	N/A	N/A	LTO5
Hewlett Packard Enterprise	Ultrium 6250 SAS	10.0.00	N/A	N/A	LTO-6 HH, SAS
Hewlett Packard Enterprise	HPE StoreEver Ultrium 15000 SAS	10.5.00	N/A	N/A	LTO-7 HH, SAS
Hewlett Packard Enterprise	HPE StoreEver Ultrium 15000 FC	10.5.00	N/A	N/A	LTO-7 HH, FC
IBM	00D8924 HH	10.0.01	N/A		LTO-6, SAS
IBM	ULT 3580-TD6	10.0.01	N/A		LTO-6, SAS
IBM	ULT 3580-HH6	10.0.01	N/A		LTO-6, SAS
IBM	IBM 3628N5X HH External	9.0.01	N/A	N/A	LTO 5, SAS
IBM	ULT 3580-TD2	6.3 sp3b	N/A	N/A	LTO2
IBM	IBM 3628L5X HH External	9.0.01	N/A	N/A	LTO 5, SAS
IBM	ULTRIUM-TD4	8.5 sp1	N/A	N/A	LTO4
IBM	IBM 49Y9898 HH Internal	9.0.01	N/A	N/A	LTO 5, SAS
IBM	TS2250	8.8.03	N/A	N/A	LTO-5
IBM	ULTRIUM-TD3	7.0 sp7c	N/A	N/A	LTO3
IBM	ULT 3580-TD4	8.5 sp1	N/A	N/A	LTO4
IBM	ULT 3580-TD3	7.0 sp7c	N/A	N/A	LTO3

IBM	TS2240 LTO4 HH	8.5 sp1	N/A	N/A	LTO4
IBM	ULT 3580	6.2 sp4b	N/A	N/A	LTO1
IBM	ULTRIUM-TD2	6.3 sp3b	N/A	N/A	LTO2
IBM	ULTRIUM-TD1	6.2 sp4b	N/A	N/A	LTO1
IBM	TS2350	8.8.03	N/A	N/A	LTO-5
IBM	TS2230 LTO3 HH	8.5 sp1	N/A	N/A	LTO3
Quantum	LTO-4	8.5 sp.1	N/A	N/A	SAS
Quantum	LTO-2 HH	8.1 sp0	N/A	N/A	half-height
Quantum	LTO-5	8.8.03	N/A	N/A	LTO5 HH SAS Standalone
Quantum	LTO-3 WORM	8.1 sp2a	N/A	N/A	
Quantum	LTO-3	8.1 sp0	N/A	N/A	
Quantum	LTO-2	8.1 sp0	N/A	N/A	
Quantum	LTO-5	8.8.03	N/A	N/A	LTO5 FH SAS Standalone
Quantum	LTO-3 HH	8.1 sp2a	N/A	N/A	SCSI, SAS, FC
Tandberg	LTO-4 FH	8.5 sp1	N/A	N/A	aka 1640LTO
Tandberg	HH LTO-4	8.5 sp2	N/A	N/A	SCSI, SAS
Tandberg	LTO-5 HH	8.8.03	N/A	N/A	SAS
Tandberg	440LTO	6.3 sp3b	N/A	N/A	IBM ULT3580-TD2
Tandberg	Tandberg LTO SAS	10.0.00	N/A	N/A	LTO-6 HH, SAS
Tandberg	TS800	8.5sp2	1	N/A	LTO3
Tandberg	820LTO	8.1 sp3a	N/A	N/A	LTO3 HH
Tandberg	HH LTO-4	8.5 sp2	N/A	N/A	SCSI,SAS
Tandberg	HH LTO 4	8.5 sp2	N/A	N/A	SCSI,SAS
Tandberg	HH LTO-2	8.5 sp2	N/A	N/A	SCSI, SAS
Tandberg	840LTO	7.0 sp7c	N/A	N/A	IBM ULT3580-TD3
Tandberg	HH LTO-3	8.5 sp2	N/A	N/A	SCSI, SAS
Tandberg	240LTO	6.2 sp4b	N/A	N/A	IBM ULT3580-TD1
Tandberg	220LTO	8.1 sp1d	N/A	N/A	
Tandberg	TS1600	8.5 sp.2	N/A	N/A	LTO4 HH
Tandberg	420LTO	7.0 sp7c	N/A	N/A	aka TS400

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
Archive	Anaconda 2750	6.2 sp1b	N/A	N/A	
Archive	Viper 60	6	N/A	N/A	
Archive	Viper 150	6	N/A	N/A	

Archive	Viper 125	6	N/A	N/A	
Archive	Viper 2525	6	N/A	N/A	
Conner	CTMS 3200	6.1	N/A	N/A	Mini QIC
Emerald	3800	6	N/A	N/A	
Emerald	4100	6	N/A	N/A	
Exabyte	2501	6	N/A	N/A	Mini QIC
PeriDAT	APD-1326	6.1	N/A	N/A	Alias for MLR1, now SLR32
Tandberg	TDC 3600	6	N/A	N/A	
Tandberg	SLR40	6.2 sp3f	N/A	N/A	20/40 GB
Tandberg	SLR140	7.0 sp5b	N/A	N/A	70/140 GB
Tandberg	SLR6/SLR24	6	N/A	N/A	12/24 GB
Tandberg	TDC 3700	6	N/A	N/A	
Tandberg	TDC 4222	6	N/A	N/A	2 GB w/compression
Tandberg	SLR75	6.2 sp3f	N/A	N/A	38/75 GB, identifies as SLR60
Tandberg	SLR60	6.2 sp3f	N/A	N/A	30/60 GB
Tandberg	SLR7	6.2	N/A	N/A	
Tandberg	SLR32/MLR1/TDC 6100	6	N/A	N/A	16/32 GB
Tandberg	TDC 4200	6	N/A	N/A	2 GB
Tandberg	SLR100	6.2 sp3c	N/A	N/A	50/100 GB
Tandberg	SLR5	6	N/A	N/A	4/8 GB
Tandberg	SLR50/MLR3	6.1	N/A	N/A	25/50 GB
Tandberg	TDC 3500	6	N/A	N/A	
Tandberg	TDC 3800	6	N/A	N/A	
Tandberg	TDC 4100	6	N/A	N/A	1 GB
Wangtek	5150	6	N/A	N/A	
Wangtek	9500 DC	6	N/A	N/A	5 GB w/compression
Wangtek	5525	6	N/A	N/A	
Wangtek	5099	6	N/A	N/A	
Wangtek	9500es	6	N/A	N/A	5 GB
Wangtek	51000	6	N/A	N/A	

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
Dell	RD1000	8.1 sp3a	N/A	N/A	Windows, Linux; USB, SATA
Hewlett Packard Enterprise	RDX	10.5	N/A	N/A	USB 3.0
IBM	RDX	8.1 sp3a	N/A	N/A	

Imation	RDX	9.0.01	N/A	N/A	SATA, USB 2.0, USB 3.0
Iomega	REV 70	8.1 sp3a	N/A	N/A	Windows: IDE,SATA,USB Linux: IDE,SATA,USB (2.6 kernel distos only) NetWare: IDE
Iomega	REV 35	7.0 sp6a	N/A	N/A	Windows only. IDE, SCSI, USB
Iomega	REV 35	8.1	N/A	N/A	Windows: IDE,SCSI,USB Linux: IDE,SCSI NetWare: IDE,SCSI
Lenovo	Lenovo RDX	8.1 sp3a	N/A	N/A	Internal USB 2.0
Prostor	RDX	8.1 sp1c	N/A	N/A	
Quantum	GoVault	8.1 sp1b	N/A	N/A	Windows, Linux (8.1 sp3a); SATA, USB (Internal, External)
Tandberg	RDX Quickstor	8.1 sp3a	N/A	N/A	Windows, Linux; USB, SATA

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
DumCo	XYZ-3000	7.0 sp7b	1	6	None

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
AIWA	TD-8001	6.2	N/A	N/A	Travan 4, SCSI
AIWA	TD-20001	6.2	N/A	N/A	Travan 5, SCSI
AIWA	TD-8000	6.2	N/A	N/A	Travan 4, SCSI
Certance	STT20000/NS20	6.2 sp3e	N/A	N/A	IDE, SCSI
Certance	Travan 40	6.3 sp1b	N/A	N/A	IDE, STT2401, STT3401
Certance	STT8000/NS8	6.1	N/A	N/A	IDE, SCSI
Certance	Travan 20 USB	6.3 sp3b	N/A	N/A	STT6201
Certance	Travan 40 USB	6.3 sp3b	N/A	N/A	STT6401
Compaq	TR4	6.3 sp1b	N/A	N/A	IDE
Conner	CTT8000	6.1	N/A	N/A	Travan 4, SCSI
Dell	PV-100T Travan40	6.3 sp2b	N/A	N/A	IDE
Exabyte	Eagle TR-4	6.1	N/A	N/A	
Tandberg	NS20	-	N/A	N/A	Travan 5 w/compression, SCSI
Tandberg	TR4	-	N/A	N/A	4 GB, SCSI
Tandberg	NS8	-	N/A	N/A	Travan 4 w/compression, SCSI
Tecmar	NS8	6.1	N/A	N/A	SCSI
Tecmar	NS20	6.2	N/A	N/A	SCSI
Wangtek	TS420	6.1	N/A	N/A	SCSI

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
OnStream	ADR2.60	6.3	N/A	N/A	

Manufacturer	Device Name	Minimum Version	Drives	Slots	Notes
Enhance Technology Inc.	Ultrastor RS16 IP-4	8.5 sp1	N/A	N/A	Disk to Disk Backup via VLD
Sony	SDZ-100	7.0 sp5b	N/A	N/A	SAIT