BackupAssist™ v8

File Archiving

User Guide

BackupAssist User Guides explain how to create and modify backup jobs, create backups and perform restores. These steps are explained in more detail in a guide's respective whitepaper.

Whitepapers should be used as the main reference documents when planning your backups and your data protection strategy. Whitepapers include important considerations, configuration explanations and the implementation information needed to use BackupAssist effectively.

Contents

1. Overview

BackupAssist File Archiving is a file-based backup that works with both disk devices (e.g. external HDDs, CD/DVDs, RDX drives, NAS, FTP servers) and tape drives with the Zip-To-Tape Add-on. Backups created using File Archiving are stored as .ZIP files that contain all of the data selected in the backup job.

Documentation

More information on File Archiving can be found in the File Archiving whitepaper.

The whitepaper contains comprehensive information and should be referred to when planning a backup strategy using BackupAssist File Archiving.

Other BackupAssist documentation can be accessed through the Documentation webpage

Recommended reading:

- To learn more about the BackupAssist Backup tab, see the BackupAssist Backup Tab User Guide.
- To learn more about the BackupAssist Restore tab, see the BackupAssist Restore Tab User Guide
- To learn more about the BackupAssist Recover tab, see the BackupAssist Recover Tab User Guide
- To learn more about the BackupAssist Settings tab, see the BackupAssist Settings Tab User Guide

Licensing

File Archiving is a standard feature included with the BackupAssist license. To back up data to a tape drive requires the *Zip-To-Tape Add-on* license, once the initial trial period has expired. Please contact your local BackupAssist reseller or distributor for pricing information, or visit www.BackupAssist.com.

For instructions on how to activate / deactivate license keys, visit our Licensing BackupAssist page.

File Archiving requirements

Item	Description of requirements
Operating systems	Windows 7, 8, Server 2008/R2, 2012/R2, SBS 2008 and 2011.
Supported hardware	Tape, external HDD, iSCSI device, NAS, SAN, optical disc (CD/DVD/Blu-Ray), RDX drive, local directory, network location and FTP server.
Tape backups	Only standalone tape drives installed on the same machine as BackupAssist are supported (excluding Travan tape drives). You cannot use an autoloader device, or a tape drive located on another machine. The tape drive you use must ship with its own set of drivers, or Windows compatible drivers must be available for download from the manufacturer's website.

2. Backup considerations

Before creating a backup job, it is important to understand what backup and restore options are available. This section provides guidance on some key considerations.

Exchange VM Detection

When backing up a Hyper-V guest with an Exchange Server, enter the authentication information for that guest into the **Exchange VM Detection** tab on the **Selection** screen when you create the job. With these credentials, BackupAssist can detect what guests have an Exchange Server, and list the EDB file available for each guest when you perform a restore using the Exchange Granular Restore console.

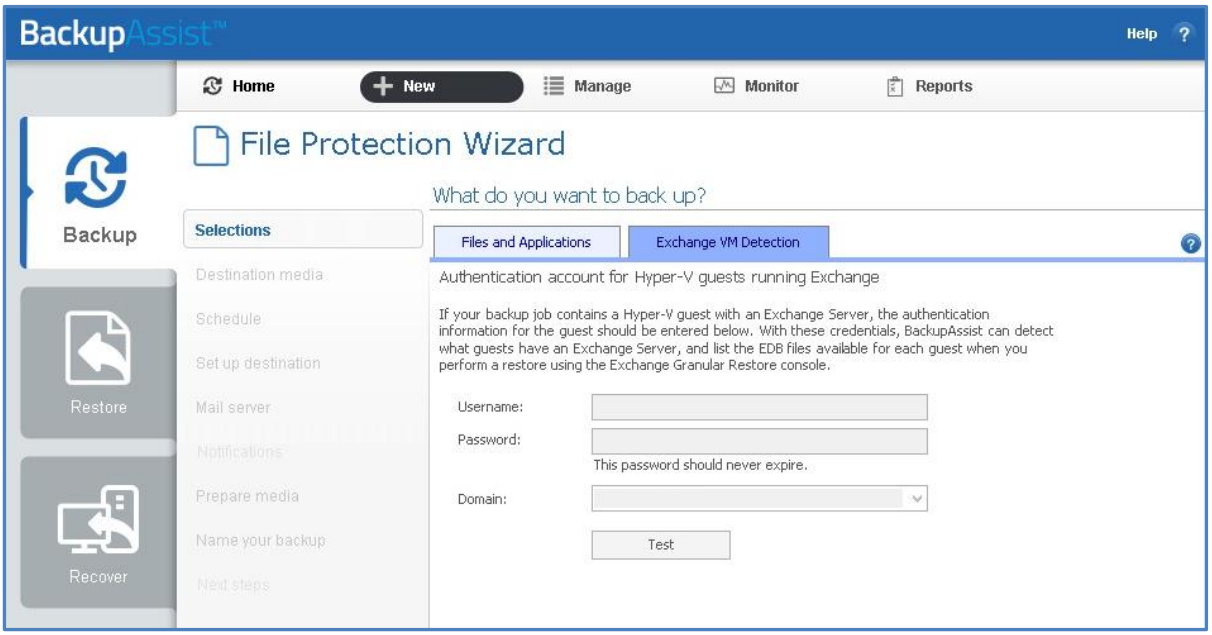

Figure 1: Selection screen - for an Exchange Server on a Hyper-V guest

The Exchange VM Detection tab will appear when the Hyper-V role is installed and running on the server. If you are backing up multiple Exchange guests, each one should have the same username and password.

The Hyper-V process is automated but the restore requires both the *Exchange Granular Restore Add-on and the Hyper-V Granular Restore Add-on* licenses.

Restore vs. Recovery

A restore is the process of accessing a backup and restoring it to the original (or a new) location, if your data is lost, corrupted or if you want an earlier version of that data. However, if your computer cannot start itself, you may need to perform a recovery.

A recovery is the process by which a computer is recovered after hardware has been replaced or an operating system failure has occurred, and your computer can no longer start itself. To perform a recovery you need a bootable media to start your computer, and an image backup that the bootable media can use to recover your operating system, data and applications.

For more information on data recovery, see the Recover tab & RecoverAssist Whitepaper.

3. Creating a File Archiving backup

The following instructions describe how to create a backup job using BackupAssist File Archiving.

Launch BackupAssist and follow the steps outlined below:

1. Select the **Backup** tab, and click **Create a new backup Job**
2. Select **File Archiving:** If this is the first time you have created a backup job, you will be asked to provide a *Backup user identity*. See the section above, BackupAssist settings, for guidance.
3. **Selections:** The selections screen is used to select the data and applications that you would like to back up. Any VSS applications detected will be displayed here as application directory containers.

   An Exchange VM Detection tab will be available if you are backing up an Exchange VM guest.

   Select the volumes, folders, files and applications that you want to back up, and click **Next.**
4. **Destination media:** The destination screen is used to select the type of media that you want to back your data up to. This step's name will change to the media type selected, when you click next.

   a. **Select a device** for your backup destination.

   b. **Select an encryption type** if you want to encrypt your backup.

   - ZIP encryption is available for all destinations. It will encrypt and password protect your backup file using 256 bit AES encryption.
   - BitLocker encryption is available for External disk or RDX drive destinations. BitLocker will encrypt the destination media. To learn about BitLocker, see our BitLocker resource page.

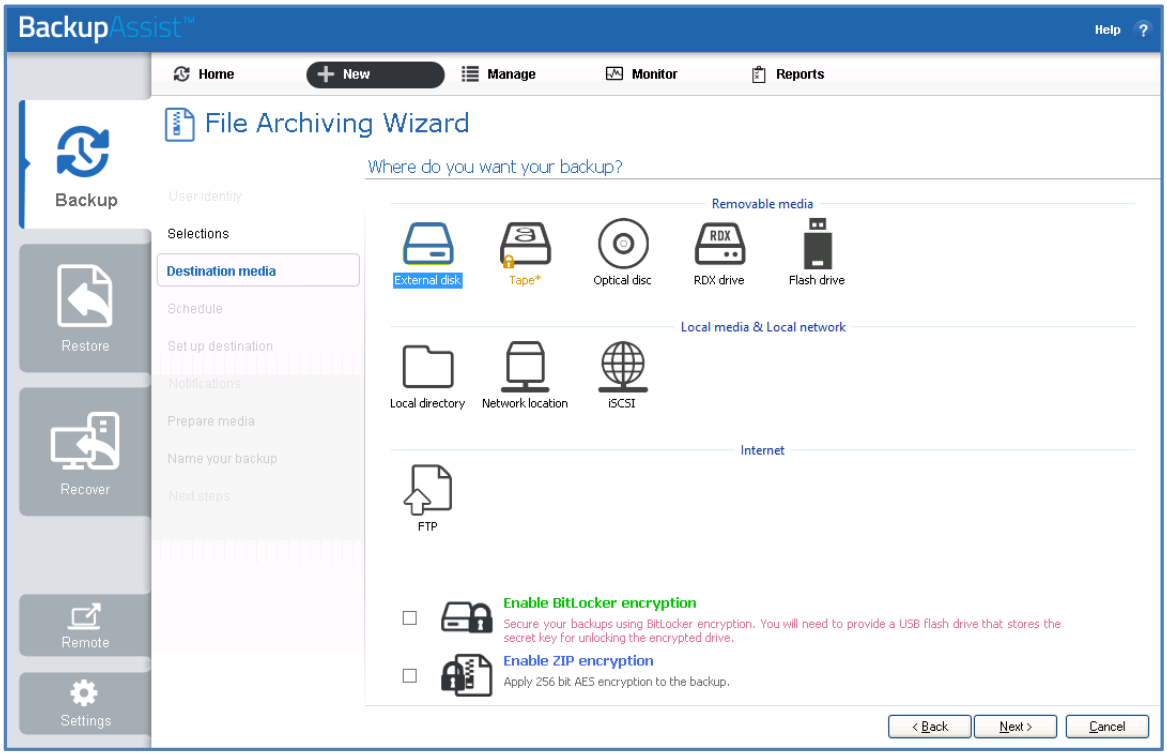

Figure 2: File Archiving backup – Destination media selection screen.

c. Click **Next.**

5. **Schedule:** This screen is used to select when and how you would like the backup job to run, and how long you would like the backup to be retained for. A selection of pre-configured schedules, called schemes, will be displayed. Select a scheme and click **Next**.

   - The schemes available will depend on the type of destination media selected in step 4.
   - Clicking on a scheme will display information about the schedule used.

   For detailed information on scheduling options and customizations, see the Backup tab user guide.

6. **Set up destination:** This screen is used to configure the location of the media selected in step 4.

   The options presented will change with the type of media selected.

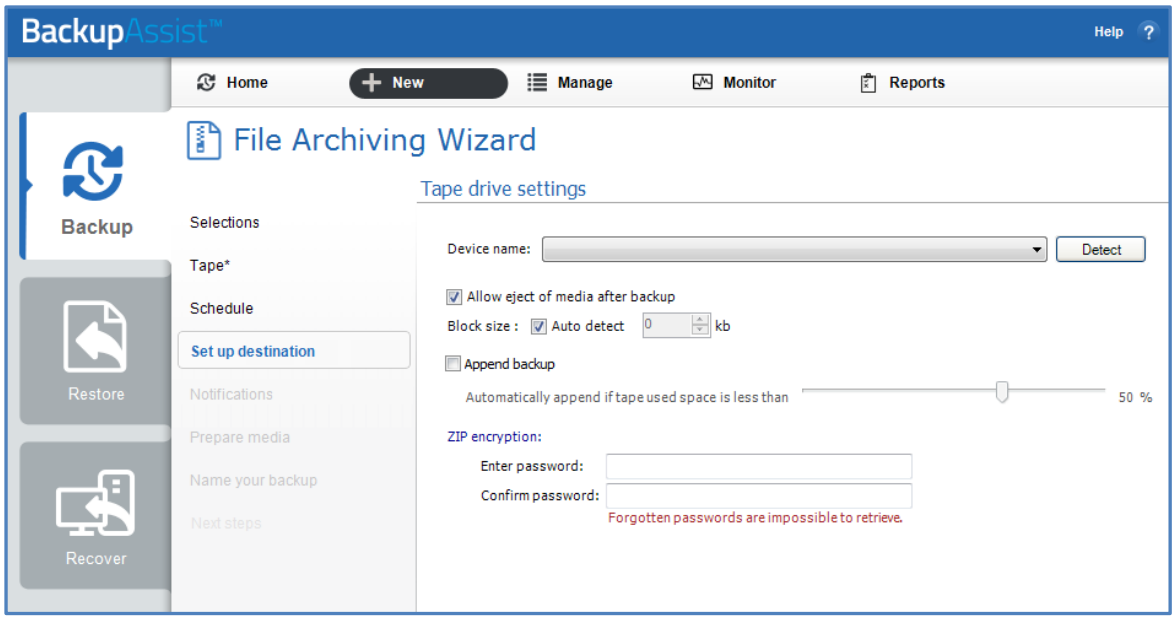

Figure 3: File Archiving backup – destination selection

- If your media is removable, you can set the media to eject after the backup job has finished.
- If you selected ZIP or BitLocker encryption, enter a password and any requested encryption information into the fields provided.

For Tape drives: If you are configuring a tape drive, the following selections are available:

a. Select the **Device name** of your tape drive from the drop-down menu.

   - If your tape drive is not listed in the drop-down menu, click **Detect.**
   - If the drive is not detected make sure you have installed the default Windows drivers for your device and try again.

b. Select **Allow eject of media after backup** if you want BackupAssist to automatically eject your tape media after each backup has been completed. This will make sure the data on the tape is not overwritten the next time a backup runs.

c. **Block size** should only be used to specify a manual block size if your tape backups are failing.

d. **Append backup** can be checked if you want subsequent backups to be added to the existing backups on the inserted tape. If *Append backup* is disabled, BackupAssist will overwrite all existing data on the tape each time a backup is run. You should only enable append if you believe your tape has enough space to accommodate at least two full backups or if you have scheduled either differential or incremental backups.

e. A **ZIP encryption** option will be available if you selected *Enable ZIP encryption* during the *Destination media* step. Add a password if you want to use backup encryption. Once encrypted, a password is required to restore your data.

> **Note:** It is important that you keep a copy of your password in a safe place, as we cannot retrieve passwords if they are lost or forgotten.

7. **Notifications**: Once a backup job has completed, BackupAssist can send an email to inform selected recipients of the result. This email notification can be enabled during the creation of a backup job, if the mail server has been configured. To enable email notifications:

   To send email notifications, you will need to configure an SMTP mail server for BackupAssist. See the Backup tab user guide for more information.

   a. Select, **Add an email report notification.**
   b. Enter recipients into the **Send reports to this email address** field.
   c. Enter recipients into the **Also send reports to this email address** field. You can then select the condition under which the email should be sent, using the drop-down box.

   After the backup job has been created, you can modify the notifications by adding and removing recipients, setting additional notification conditions and including print and file notification types.

   To learn more about notification options, see the Backup tab whitepaper.

   Prepare media: If you selected a portable media as your backup destination you will be given the option to prepare the media for BackupAssist. BackupAssist will write a label onto the media so that it can recognise what media has been attached, and determine if it is the correct media for your backup schedule.

   To enable media detection:

   a. Select, **Let BackupAssist keep track of your media.**
   b. Select what you would like BackupAssist to do, *if the wrong media is inserted*.
   c. Select what you would like BackupAssist to do, *if new or unrecognized media is inserted*.

   BackupAssist will display all removable media that is currently attached, along with a text field and drive designation drop-down box, which can be used to provide a label for the media.

   To prepare your media:

   a. Enter the name and drive designation to be used for each media device listed.
   b. Select **Prepare** for each media device listed.

   If you are using BitLocker, refer to the BitLocker resource page for disk preparation guidance.

8. **Name your backup:** Provide a name for your backup job, and click **Finish**.

▶ **The File Archive Backup job has now been created.**

Important: Once a **backup job** has been created, it should be reviewed and run using the *Manage* menu. This menu provides additional options to configure your backup. See the section, File Archiving backup management, for more information.

Important: Once the *backup* has been created, it should be checked. You can check the backup by performing a manual test restore, or using the Backup Verification feature. A manual restore is the only way to fully test a backup, and regular manual restores should be part of your backup solution.

4. Restoring from a File Archiving backup

This section provides instructions on how to restore data that was backed up using BackupAssist File Archiving.

To restore data from a **File Archiving** backup, start BackupAssist and follow these steps:

1. Select the **Restore tab**

   The *Restore tab* has a *Home page* and a *Tools menu*. The *Home page* is the default screen and the recommended starting point for performing a restore. The *Tools menu* should only be used by experienced administrators or users being assisted by technical support.

2. From the **Home page**, select the type of restore you want to perform.

   - *Files and folders* will display all data backups and all VSS application backups.
   - *Applications* will display backups that contain VSS applications, and exclude data only backups.
   - *Exchange*, *SQL* or *Hyper-V*, will display all backups that contain the selected application. Selecting an application type will display application specific restore tools (e.g. Hyper-V Granular Restore and SQL Restore) as well as the Restore Console.

3. Once you have selected the type of restore you want to perform, the *Home page* will display all catalogued backups that match your selection. The backups displayed will be for active backup jobs, and grouped by the source data's location and the restore tool that can be used.

   - If a backup can be used by two restore tools, it will appear in two groupings.
   - If a backup contains data from multiple locations, it will appear in a grouping for each location.

   If your backup included both data and VSS applications, both will be available to restore once the backup has been loaded in step 4, regardless of the restore type selected.

   Select the **Restore Console.**

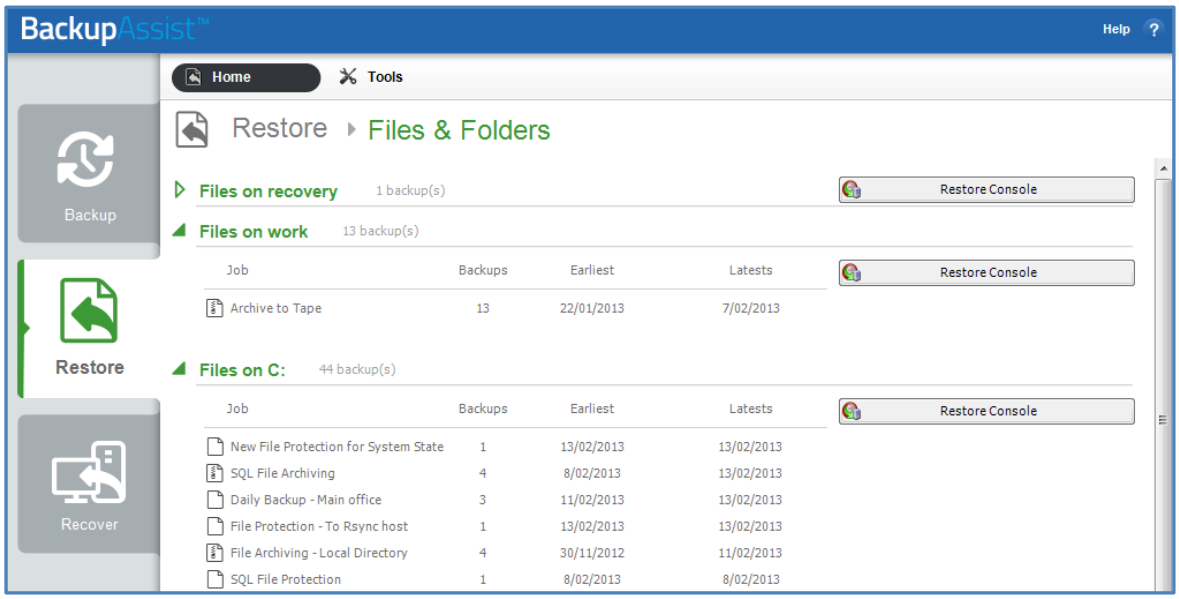

Figure 4: BackupAssist Home page – selection results

4. **Restore Console – backup and data selection**

The BackupAssist *Restore Console* will open and load all of the backups that were listed on the *Home page*. The next step is to locate the data you want to restore, from the loaded backups.

The Restore Console provides two tools to locate your data:

- The **Browse** tab. Select this tab if you know the backup and date you wish to restore from, or if you need to restore an entire backup set.
  a. Use the drop-down menu to choose the backup that you want to restore from.
  b. Use the calendar to select the date you want to restore from.
  c. Use the middle panes to expand the backup set.
  d. Select the data to restore.
  e. Click **Restore to** at the bottom right of the window.
- The **Search** tab. Select this tab to search all of the loaded backups for the data you want to restore. You can display data filtered by name, date, size and type, for all backups. The results can be compared (e.g. the dates of two files) to identify the correct data selection.
  a. Enter your search term (The search accepts wild card searches, such as **.log* or **.doc*).
  b. Select a filter/s if required.
  c. Click the *Search* button.
  d. Select the data to restore.
  e. Click **Restore to** at the bottom right of the window.

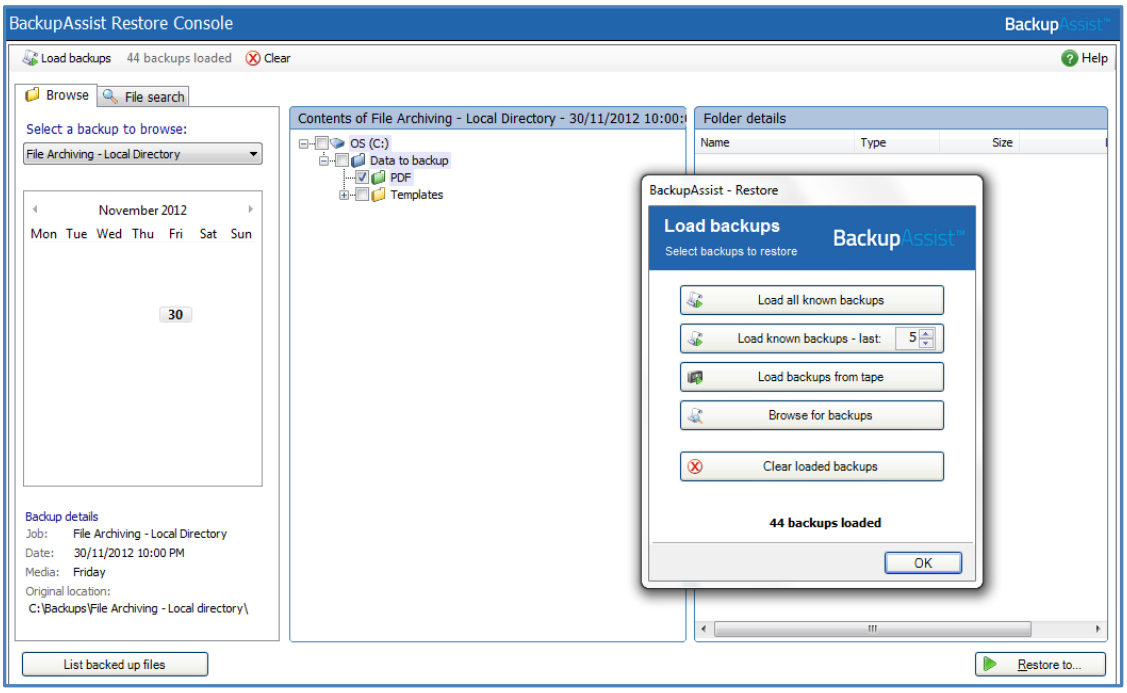

Figure 5: BackupAssist Restore Console – backup and data selection

If you wish to load backups for deleted backup jobs and for other backup groupings on the Home page, select *Load backups* and then *Load all known backups*.

For more information about data selection, refer to the Restore tab whitepaper.

5. **Restore Console – backup destination selection.**

   When you select *Restore to,* a window will open showing the *Backup location,* the *Restore to* destination and the *Restore options*.

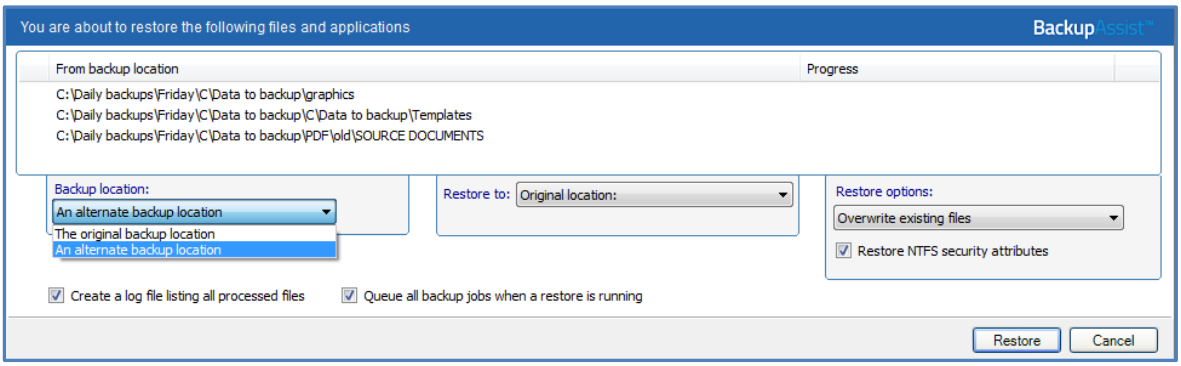

Figure 6: BackupAssist Restore Console – restore destination

   a. Review **Backup location:** Change the selection if the backup was moved after it was created.

   b. Review **Restore to:** Leave the *Original location* selected or chose an *Alternative path*.

      Restoring to an alternate location will use a minimal path. For example, restoring a single file to an alternate location will copy the file to the location without re-creating the original folder structure.

   c. Review the **Restore options:**

      - Select *Overwrite all existing files*, *Do not overwrite existing files* or *Only overwrite older files*.
      - The option, *Restore NTFS security attributes* will be selected by default.

   d. Selecting *Create a log file listing all processed files*, will create a file that lists the success or failure of each file. The log is opened by selecting the log file's link in the backup report.

   e. *Queue all backup jobs when a restore is running*, is selected by default.

   f. Click the **Restore** button to restore your data.

      If BackupAssist cannot access the backup location you will be prompted to either connect the appropriate media or specify an alternate location where the backup can be found.

      The restore will run from the destination window and a **Report** link will appear once the restore has finished.

   g. Select **Done**.

▶ **Your File Archive restore has now been completed.**

Important: The Restore Console can restore encrypted files, but you will need to supply the password. It is important that you keep a copy of your password in a safe place, as we cannot assist you with opening password encrypted files if your password is lost or forgotten.

Helpful hint: These instructions explain how to restore data using the *BackupAssist Restore console*. If you do not have BackupAssist installed and need to restore a *File Archive* backup, you can browse to the location of your backup using Windows Explorer and copy the required files to any location, as long as the files are not encrypted.

Helpful hint: If you are having problems performing a restore from a tape media, you can attempt to perform the restore using the **Retrieve Backup from Tape** tool, under the **Tools menu**. This tool will directly access the tape media, unlike the Restore Console which loads all backups. The *Retrieve Backup from Tape* tool will restore the entire contents of the tape. It cannot restore individual items.

5. File Archiving backup management

Once you have created a backup job, you can modify the settings and access advanced configuration options using the *Manage* menu.

To access the backup management screen:

1. Select the BackupAssist, **Backup tab.**
2. Select **Manage** from the top menu. A list of all backup jobs will be displayed.
3. Select the backup job you want to modify, and select **Edit.**
4. Select the required configuration item on the left. Key configurations are described below.

To learn more about the backup management options, see the Backup tab whitepaper.

Manually running a backup job

All new and modified backup jobs should be manually run to ensure they work as intended.

1. Select the backup job, and select *Run*.
2. You will be prompted to *Rerun a past backup* or to *Run a future backup now*.
3. When the backup job starts, the screen will change to the *Monitor* view.
4. Once the backup has been completed, select the *Report* button and review the results.

Scheduling

Selecting *Scheduling* will display the **Scheduling options.** You can use this screen to change the default time and days of your scheme's daily backups. If you selected a scheme with archive backups (e.g. weekly, monthly), you can specify when each archive backup will run. The current scheme is shown, along with two pop-up menus: *Select a new schedule* and *Customize schedule*.

Select a new Schedule: This will display the pre-configured backup schemes that you chose from during the creation of your backup job. The selections available will depend on the type of destination media you have selected. You can select a different scheme using this option.

Customize schedule: This selection can be used to modify each backup within your current schedule. The default *Method* is a *Full* backup, but you can also select *Incremental*, *Differential* and *Copy*.

- **Full** means all data selected is backed up and each file is marked as having been backed up (the archive bit is cleared). To restore all your data you only need the most recent *Full* backup.
- **Differential** means only data that has changed since the last full backup is copied to the backup device. Files are not marked as having been backed up. You will require the last *Full* backup as well as the last *Differential* backup to restore your data.
- **Incremental** means only data that has changed since the last backup is copied to the backup device. Files are marked as having been backed up. You will require the last *Full* backup as well as the all *Incremental* backups since the last *full* backup to perform a complete restore.
- **Copy** is the same as a *Full* backup except that files are not marked as having been backed up. Copy backups are useful if you have multiple jobs and need to back up certain files between *Full* and *Incremental* backup runs.

For additional information on *Methods* and *Scheduling*, please refer to the Backup tab whitepaper.

Zip options

This menu can be used to enable and configure specific archiving options including compression, encryption, compression / encryption threads and NTFS security attributes.

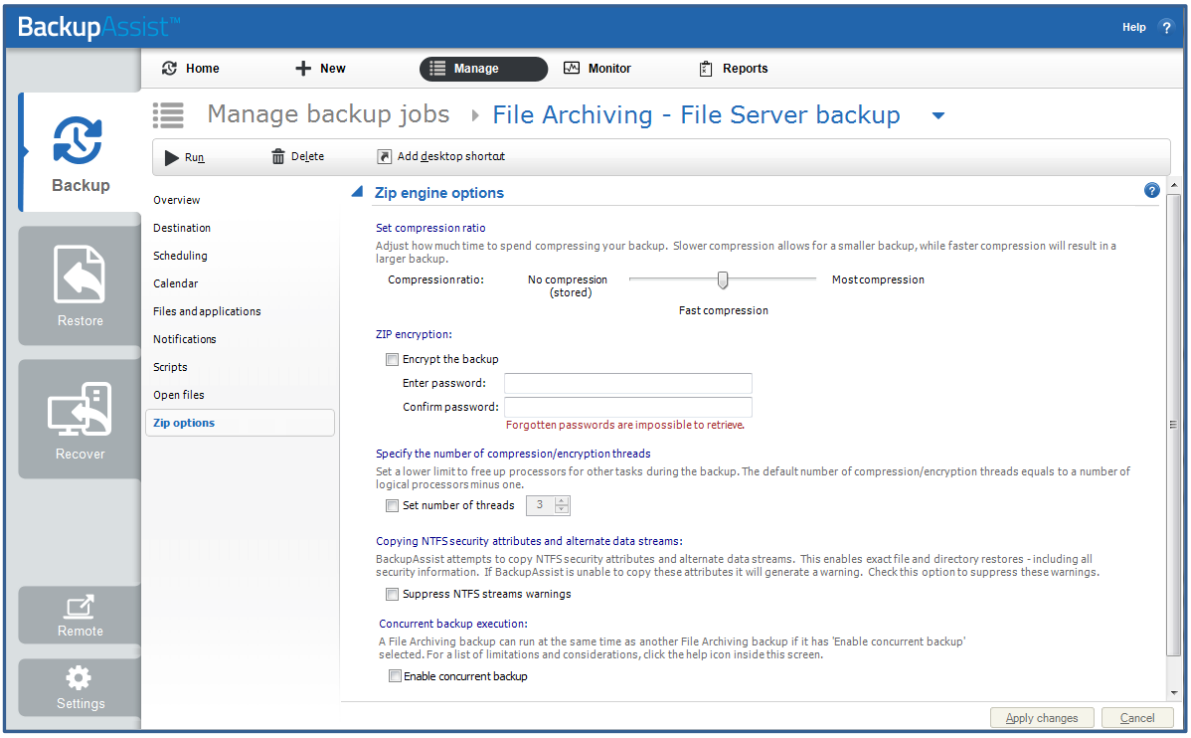

Figure 7: Archive backup options screen

Set compression ratio

Drag the slider to *No compression* for faster backups but larger backup size, or to *Most compression* for smaller backup size but longer backup times. *Fast compression* is recommended because it is faster than *Most compression* and the difference in storage savings between the two settings is minor. Enabling compression means you will save disk space on the backup destination and, as a result, store more backups on each disk drive or backup media.

ZIP Encryption

Enable if you need to make sure that your data is secure. BackupAssist will apply 256-bit AES encryption to a password protected backup file. Once encrypted, a password is required to restore your data. It is essential that you use a password that you can easily remember. Check *Encrypt the backup*, then enter and confirm a password.

AES-256 encryption is an industry-standard algorithm for encryption, which uses a 256-bit key to provide an almost infinite number of possible combinations. Estimates suggest that it could take a minimum of 30 years to crack an AES-256 encrypted file. In other words, your data is well protected with AES-256 encryption.

Specify the number of compression/encryption threads

On a multi-core or multi-processor computer, BackupAssist can use multiple threads to compress and encrypt files. This significantly reduces the time required to perform a backup. By default, BackupAssist will use one thread for each processor core on your machine minus one (e.g. 3 threads on a dual processor, dual core machine). Only modify the setting if you experience performance issues.

To alter the default BackupAssist setting for thread usage check **Manually force thread count** and enter the number of threads BackupAssist should use when compressing data.

With multi-threading, your processor is able to perform multiple tasks simultaneously, which shortens the overall time taken to complete a backup. The following table compares the performance of WinZip with BackupAssist's Archiving engine.

Copy NTFS attributes and alternate data streams

By default BackupAssist will store NTFS security attributes and alternate data streams of directories within your archive backup. Doing so means you are able to restore exact copies of your original data, including all security information. BackupAssist will try and store NTFS security attributes and alternate data streams that are set in the original source files and backed up to ZIP. If the NTFS attributes cannot be kept, a warning will appear in the backup report. File Archiving can preserve the following NTFS attributes at the file destination: Windows File Attributes, Creation time, Last modified time, NTFS security (ACLs) and NTFS alternate data streams (ADSs).

Uncheck *Suppress NTFS stream warnings*, if you prefer not to be notified in your backup report if NTFS attributes have been maintained.

Concurrent backup execution

This feature allows two backup jobs to run at the same time.

Concurrent backup combinations:

- Two File Archiving backup jobs can run at the same time if both have 'Enable concurrent backup' selected.
- An SQL Protection or Mailbox Protection backup job, with 'Enable concurrent backup' selected, can run concurrently with a System Protection, File Protection or File Archiving backup job. The File Archiving backup job does not need to have 'Enable concurrent backup' selected. (System Protection and File Protection do not have an 'Enable concurrent backup' option).
- An SQL Protection and a Mailbox Protection backup job can run at the same time, in any combination, if both have 'Enable concurrent backup' selected.
- In all cases, only two backup jobs can run concurrently.

Concurrent backup considerations:

- If two concurrent backups are scheduled to start at the same time, one backup will start first and begin preparing the job. Once the preparation phase has completed, the second backup will start
- If a third scheduled backup job has 'Enable concurrent backup' selected, it will be queued and run once one of the two existing concurrent backup jobs has finished.

Concurrent backup limitations:

- Only two backup jobs can run concurrently.
- Concurrent backups cannot write to the same destination device (e.g. local drive, NAS, RDX etc.).
- If another backup job is already running when the concurrent backups are scheduled to start, then one of the concurrent backups will start if it meets the criteria defined in the concurrent combinations section.
- A backup job cannot run concurrently if it is backing up a Hyper-V environment or an Exchange server using VSS (VSS enabled).