BackupAssist™ v9

File Archiving

User guide

Contents

1. Introduction

File Archiving
For keeping archives
Method: ZIP64
Backup to Disk / iSCSI / NAS / Tape / Blue-ray...

BackupAssist File Archiving is a file-based backup that works with both disk devices (e.g. external HDDs, CD/DVDs, RDX drives, and NAS devices) and tape drives, with the Tape Archiving Add-on.

Backups created using File Archiving are stored as .ZIP files that contain all of the data selected in the backup job. This user guide outlines how File Archiving works, and how to create and restore File Archiving backups using BackupAssist.

Documentation

This user guide provides a comprehensive guide to BackupAssist File Archiving and can be used in conjunction with other BackupAssist guides.

- For information on the BackupAssist Backup tab, see the Backup Tab user guide
- For information on the BackupAssist Restore tab, see the Restore Tab user guide
- For information on BackupAssist's settings see the Settings tab guide

Licensing

File Archiving is a standard feature included with the BackupAssist license. To back up data to a tape drive requires the *Tape Archiving 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
Supported hardware	Tape, external HDD, iSCSI device, NAS, SAN, optical disc (CD/DVD/Blu-Ray), RDX drive, local directory, network location.
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. File Archiving product overview

File Archiving features

The following features are unique to BackupAssist File Archiving and are not available in other third-party applications, such as WinZip:

- ✓ **Multi-threaded compression**

  On a multi-core or multi-processor computer, BackupAssist uses multiple threads to compress and encrypt files. This significantly reduces the time required to perform a backup.

- ✓ **Volume Shadow Copy Service (VSS) support**

  Volume Shadow Copy Service is used by Windows to take a snapshot / copy of the data used by a VSS application so that it can be backed up while the application is running. BackupAssist is VSS-aware so File Archiving backups can detect VSS applications such as Exchange, SQL, Hyper-V and SharePoint.

- ✓ **Full, Differential, Incremental and Copy backups**

  Configure your backup jobs to run full, incremental, differential and copy backups. Every time a File Archiving job runs, BackupAssist will check the archive bit of each file selected and take the appropriate action according to the type of backup scheduled. This means you can use inbuilt rotation schemes like "Full plus incremental", or create your own personalized schedules.

- ✓ **NTFS security attributes**

  The NTFS security attributes and alternate data streams of directories and files are stored within your File Archive backups. Both will be preserved if you restore your files and directories using the Integrated Restore Console.

- ✓ **Integrated Restore Console**

  BackupAssist comes with its own Restore Console, which helps you restore files and directories from a File Archive backup, including backups to tape. The Restore Console also allows you to search for specific files to restore. You can even select which version of a file to restore if the same file is located in multiple backup sets.

- ✓ **Original paths**

  The full original path of selected data is preserved in the File Archive backup.

- ✓ **Intelligent compression**

  BackupAssist automatically determines the compression level for each type of file selected for backup. If a file is not compressible (a JPEG file, for example) BackupAssist will simply store it in the archive rather than attempt to compress it first. This reduces the backup time, as BackupAssist only compresses files that actually benefit from compression.

Advantages of BackupAssist File Archiving

- ✓ **Open .ZIP format**

  Backups are stored as .ZIP files, an open file compression format supported by all Windows operating systems. Backup data stored in a .ZIP file can be accessed from any Windows machine using the built-in support for ZIP files, or with a third-party software program (if the files are not encrypted).

- ✓ **Real-time software compression**

  Data selected for back up is compressed in real time, which saves storage space and means you can store more backups on each backup drive or tape.

- ✓ **AES encryption**

  Backups can be protected with a password using 256-bit AES encryption.

- ✓ **Unlimited backup size**

  The File Archiving engine compresses backups using the ZIP64 format, so there are no restrictions on the size of an individual backup, or on the number of files that can be stored in a single .ZIP archive. ZIP64 is only supported in the native ZIP feature in Windows 7, 8 and Windows Server 2008/R2, 2012/R2. The Integrated Restore Console can access ZIP64 backups on previous version of Windows

File Archiving limitations

- **Compression and encryption can compromise backup speed**

  If both a high level of compression and the option to encrypt the backup with a password have been selected, the speed of backups may be compromised. If your backups take a long time to complete, try lowering the compression ratio or disabling encryption in the *Zip options* section of the Backup tab's *Manage* screen.

- **No support for spanning**

  Spanning a File Archiving backup across multiple .ZIP files is not supported. The backup destination you choose for your backups must have enough free space to store the entire backup as a single .ZIP file.

- **No tape autoloader support**

  File Archiving only supports backups to standalone tape drives. The use of autoloaders for a multiple tape backup rotation is not supported.

- **No remote tape backups**

  You cannot use the File Archiving engine to back up to a tape drive located on another machine (i.e. remotely).

- **Travan tape drives**

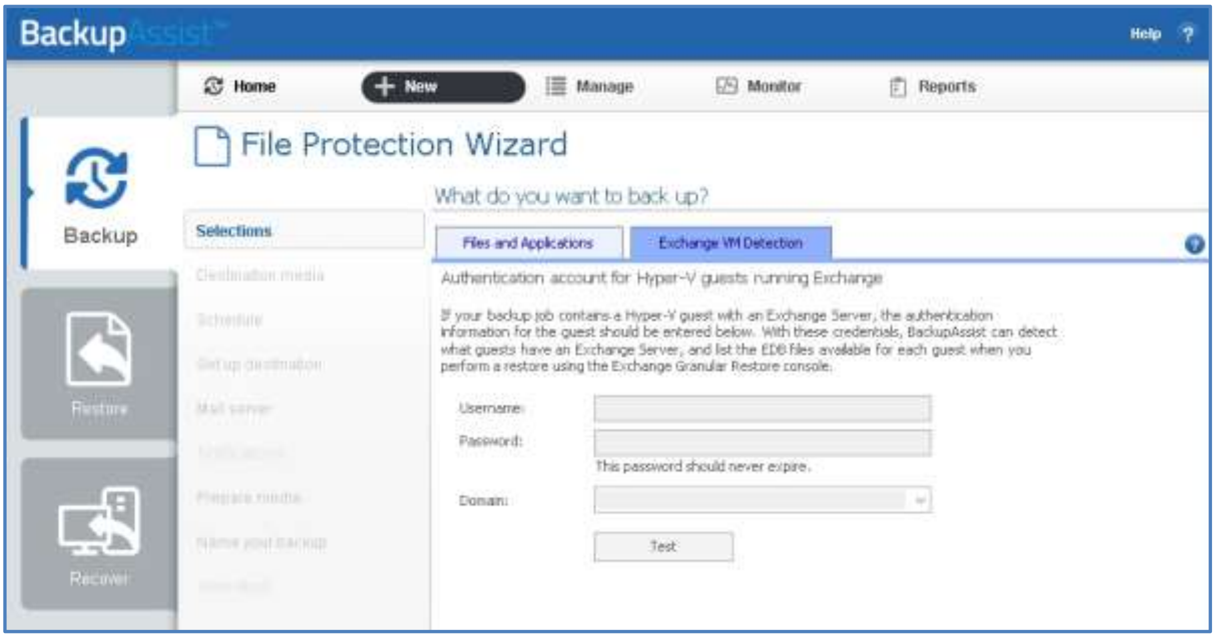
  BackupAssist does not support Travan tape drives.

3. 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.



What do you want to back up?

Authentication account for Hyper-V guests running Exchange

If your backup job contains a Hyper-V guest with an Exchange Server, the authentication information for the guest should be entered below. With these credentials, BackupAssist can detect what guests have an Exchange Server, and list the EDB files available for each guest when you perform a restore using the Exchange Granular Restore console.

Username:

Password:

This password should never expire.

Domain:

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 Add-on* and the *Hyper-V Advanced 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 System Recovery guide

4. BackupAssist settings

When creating a backup job, there are some global settings that should be configured in BackupAssist. If they are not configured, you will be prompted to complete them during the creation of your first backup. It is recommended that this is done in advance.

BackupAssist's settings can be entered and modified using the selections available in the **Settings tab.** Clicking on the *Settings* tab will display the selections as icons. Four of these are used when creating new a backup job and each one is described below:

Backup user identity

Backup jobs require an administrator account with read access to the data source, and full read-write access to the backup's destination. It is recommended that a dedicated backup account is created for this purpose. The account's details are entered here and your backup jobs will be launched using these credentials. The account's permissions will be validated both when the backup user identity is entered and when the job is executed. If no account is specified or the account has insufficient permissions, the backup job will fail and note the error in the backup report.

A video explaining the creation of a backup user identity can be found on our, Videos Webpage.

Email server settings

This menu item is used to enter the details of the SMTP server used by BackupAssist to send email notifications. The SMTP server must be configured if you want to have an email *Notifications* step enabled when you create a backup job.

Email address list

This menu item is used to define and store the email addresses of potential notification recipients. The list will be used to populate the recipient selection screen when configuring an email notification for a backup job. Any email addresses entered during the creation of a new notification are automatically added to the *Email address list*.

Network paths

This option allows you to enter access credentials for networks, domains and drives that the default account (specified in the *Backup user identity)* does not have access to. Enter or browse to the location and add it to the *Path list*. The *Edit* option will allow you to enter an authentication account, specifically for that path. When you create a backup job to a remote location, that location will be automatically added here.

Having multiple connections to a resource using the same logon credentials can generate a Windows error, such as the BA260 NAS error. It is therefore recommended that you avoid having mapped shares on the computer running BackupAssist that are the same as the paths configured in BackupAssist.

5. 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**

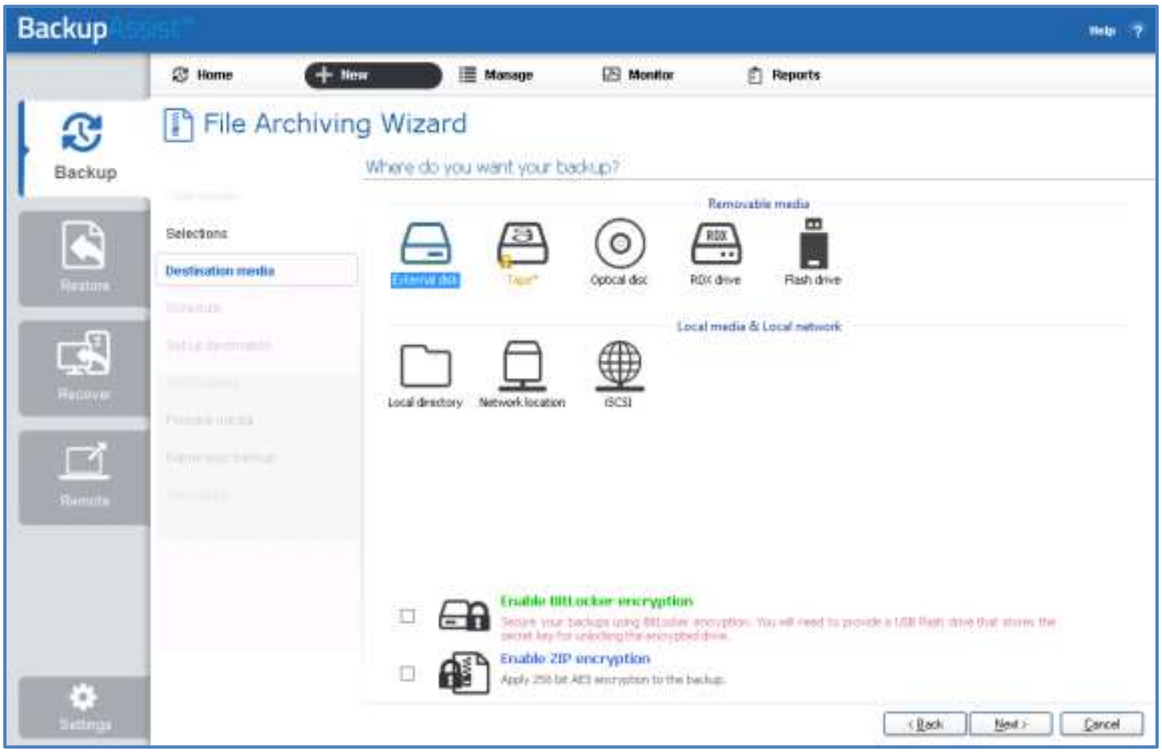
   The selections screen is used to select the data and applications that you would like to back up. Any VSS applications detected will be displayed here as application directory containers.

   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.



File Archiving Wizard

Where do you want your backup?

□ Enable BitLocker encryption
Secure your backups using BitLocker encryption. You will need to provide a USB flash drive that stores the secret key for unlocking the encrypted drive.

□ Enable ZIP encryption
Apply 256 bit AES encryption to the backup.

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

   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.

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.

The scheme full plus incremental is only available when backing up to an external hard drive, but you can modify the schedule to force this type of backup, after the backup job has been created.

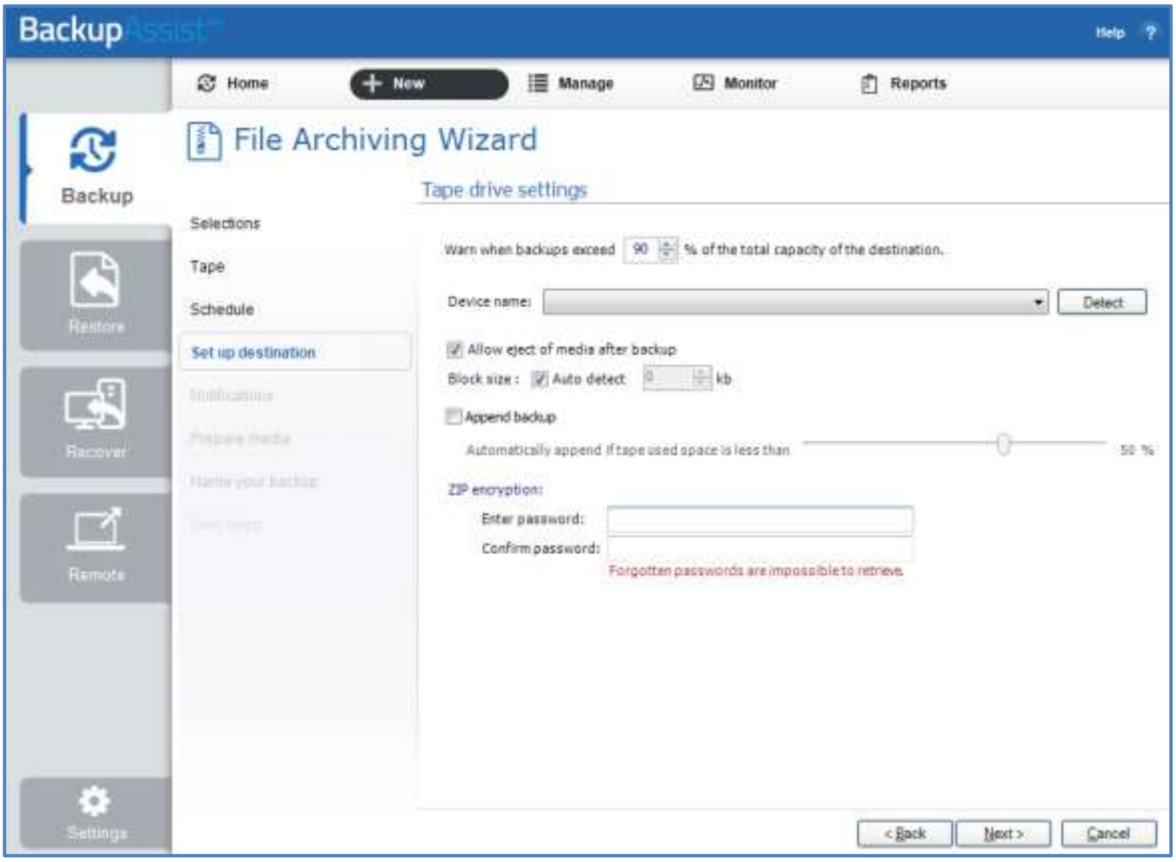
For detailed information on scheduling options and customizations, see the Backup tab guide.

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.

If you are using a *Local media & Local network* destination, a *Check destination* button will be available to check your backup destination for possible problems. After the checks have been completed, the results can be viewed by selecting the *Report* link. If you are using *Removable media* destinations, these checks are performed when you select *Prepare* on the *Prepare Media* step.



File Archiving Wizard

Tape drive settings

Warn when backups exceed 90 % of the total capacity of the destination.

Device name:

☑ Allow eject of media after backup

Block size : ☑ Auto detect 0 kb

□ Append backup

Automatically append if tape used space is less than 50 %

ZIP encryption:

Enter password:

Confirm password:

Forgotten passwords are impossible to retrieve.

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.

> **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.

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.

If you have more than one tape drive installed and want to back up to multiple drives, you will need to create a separate backup job for each drive

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:

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 user guide]()

To send email notifications, you will need to configure an SMTP mail server for BackupAssist. See the [BackupAssist settings section]() to learn more or the [Backup tab user guide]() for instructions.

8. **Prepare media**

If you selected a portable media device as your backup destination, you will be given the option to prepare and label the media. The label allows BackupAssist to recognize the media and ensure that the correct media is being used on the correct day.

For example, if you put an RDX drive in on Tuesday but it was labelled Wednesday, BackupAssist will warn you that the incorrect media has been detected.

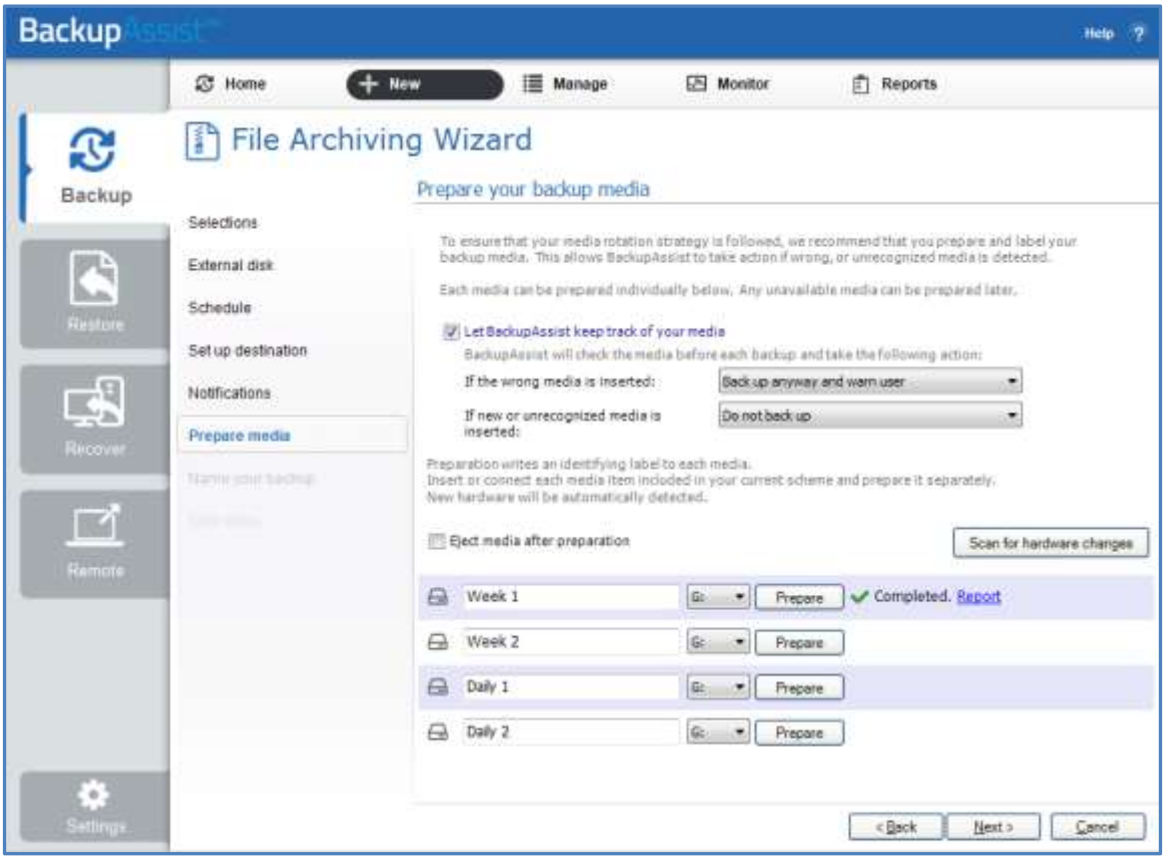
To enable media detection:

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.



File Archiving Wizard

Prepare your backup media

To ensure that your media rotation strategy is followed, we recommend that you prepare and label your backup media. This allows BackupAssist to take action if wrong, or unrecognized media is detected.

Each media can be prepared individually below. Any unavailable media can be prepared later.

☑ Let BackupAssist keep track of your media

BackupAssist will check the media before each backup and take the following action:

If the wrong media is inserted: Back up anyway and warn user

If new or unrecognized media is inserted: Do not back up

Preparation writes an identifying label to each media.
Insert or connect each media item included in your current scheme and prepare it separately.
New hardware will be automatically detected.

☐ Eject media after preparation

Scan for hardware changes

Week 1	G:	Prepare	✓ Completed. Report
Week 2	G:	Prepare	
Daily 1	G:	Prepare	
Daily 2	G:	Prepare	

Figure 4: File Archiving backup – Prepare 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.

Selecting *Prepare* labels the backup media and adds a link to a *Destination Check report*. The report will advise if any problems were detected with the backup media.

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

9. **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.

6. Restoring from a File Archiving backup

The Restore tab displays the restore options available. This section provides instructions on how to use the *Local and Network Files* restore option, which is used to restore files and folders and VSS applications that do not have their own specific restore option.

The other restore options are documented in technology specific guides, as follows:

- For *Hyper-V Host File* and *Hyper-V Granular* restore, see the Hyper-V Protection guide.
- For *SQL Server* and *SQL Point-in-Time* restores, see the SQL Protection guide
- For *Exchange Server* and *Exchange Granular* restores, see the Exchange Protection guide

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

1. **Select the Restore tab**

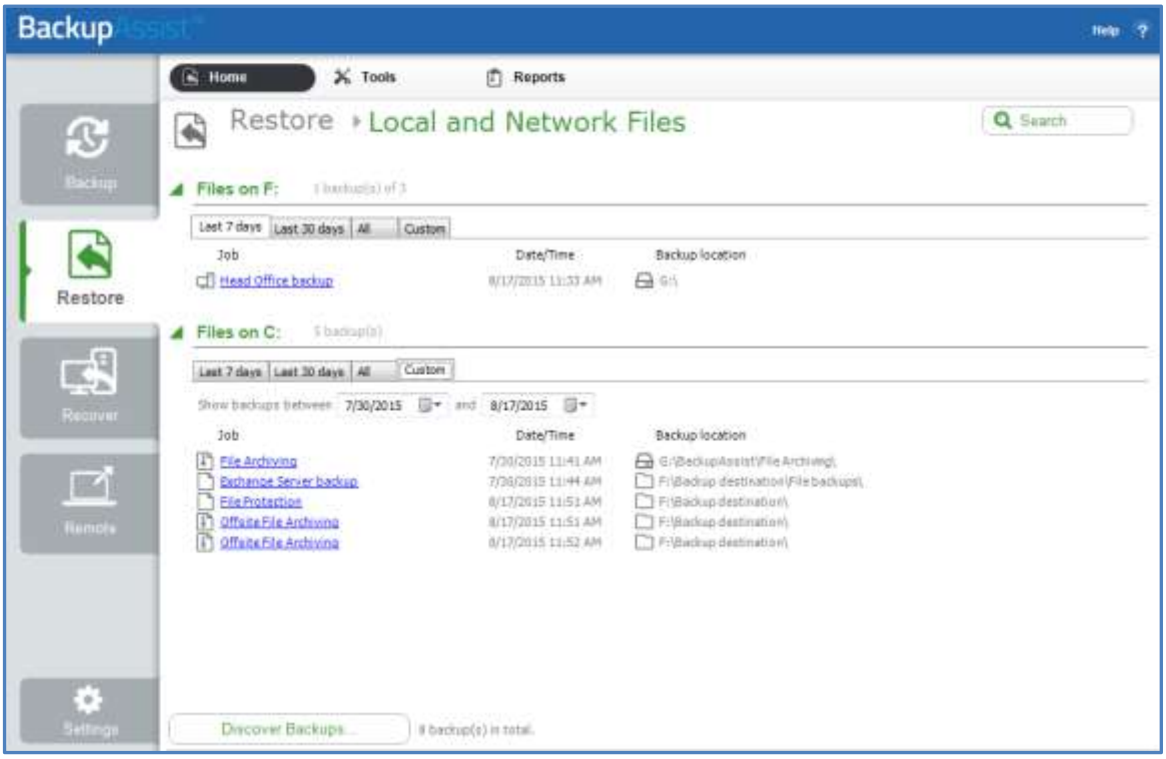
   The *Restore tab* has a *Home page* and a *Tools page*. The *Home page* is the default page and the recommended starting point for performing a restore. The *Tools page* should only be used by experienced administrators or users being assisted by technical support.

2. **Select Local and Network Files**

   This will display the volumes backed up by this installation of BackupAssist. It can also show backups from other machines added using the *Discover Backups* button.

   Expand a volume to display all of the backups available for that volume. There are tabs above each volume's backup list to help locate the required backup.

   - The *Last 7 days* and *Last 30 days* tabs can be used to display the backups within those ranges.
   - The *Custom* tab allows you to select a specific date range and display backups for that period.



Restore ▸ Local and Network Files

Files on F: 1 backup(s) of 1

Last 7 days | Last 30 days | All | Custom

Job	Date/Time	Backup location
Head Office backup	8/17/2015 11:33 AM	G:\

Files on C: 5 backup(s)

Last 7 days | Last 30 days | All | Custom

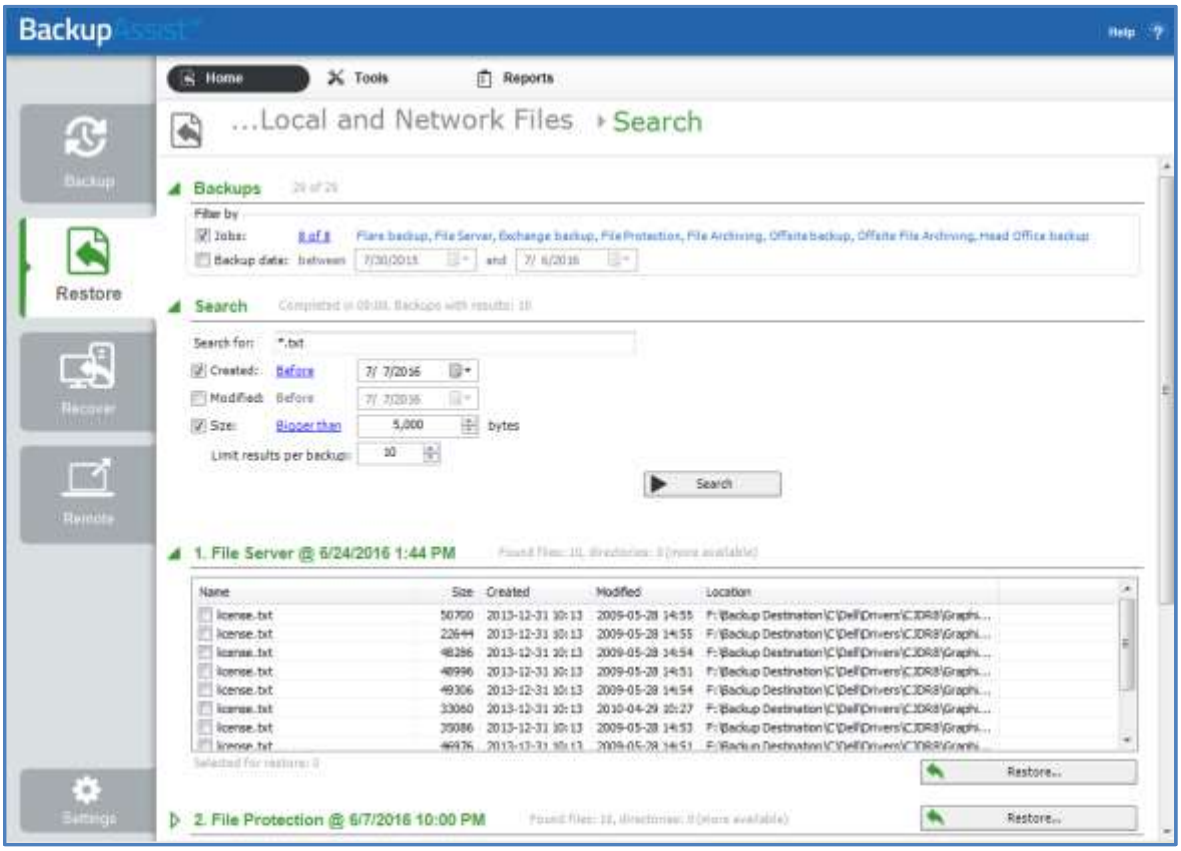
Show backups between 7/30/2015 and 8/17/2015

Job	Date/Time	Backup location
File Archiving	7/30/2015 11:41 AM	G:\BackupAssist\File Archiving\
Exchange Server backup	7/30/2015 11:44 AM	F:\Backup destination\File backups\
File Protection	8/17/2015 11:51 AM	F:\Backup destination\
Offsite File Archiving	8/17/2015 11:51 AM	F:\Backup destination\
Offsite File Archiving	8/17/2015 11:52 AM	F:\Backup destination\

8 backup(s) in total.

Figure 5: Restore tab – backup selection

The **Search** button allows you to locate files to restore across multiple backups. When you select Search, the Restore console will display the Search page.



...Local and Network Files › Search

Backups 20 of 20

Filter by

☑ Jobs: 8 of 8 Flare backup, File Server, Exchange backup, File Protection, File Archiving, Offsite backup, Offsite File Archiving, Head Office backup

□ Backup date: between 7/30/2015 and 7/ 6/2016

Search Completed in 00:00. Backups with results: 10

Search for: *.txt

☑ Created: Before 7/ 7/2016

□ Modified: Before 7/ 7/2016

☑ Size: Bigger than 5,000 bytes

Limit results per backup: 10

▶ Search

1. File Server @ 6/24/2016 1:44 PM Found files: 10, directories: 0 (more available)

Name	Size	Created	Modified	Location
□ license.txt	50700	2013-12-31 10:13	2009-05-28 14:55	F:\Backup Destination\C\Dell\Drivers\CJDR8\Graphi...
□ license.txt	22644	2013-12-31 10:13	2009-05-28 14:55	F:\Backup Destination\C\Dell\Drivers\CJDR8\Graphi...
□ license.txt	48286	2013-12-31 10:13	2009-05-28 14:54	F:\Backup Destination\C\Dell\Drivers\CJDR8\Graphi...
□ license.txt	48996	2013-12-31 10:13	2009-05-28 14:51	F:\Backup Destination\C\Dell\Drivers\CJDR8\Graphi...
□ license.txt	49306	2013-12-31 10:13	2009-05-28 14:54	F:\Backup Destination\C\Dell\Drivers\CJDR8\Graphi...
□ license.txt	33060	2013-12-31 10:13	2010-04-29 10:27	F:\Backup Destination\C\Dell\Drivers\CJDR8\Graphi...
□ license.txt	35086	2013-12-31 10:13	2009-05-28 14:53	F:\Backup Destination\C\Dell\Drivers\CJDR8\Graphi...
□ license.txt	46976	2013-12-31 10:13	2009-05-28 14:51	F:\Backup Destination\C\Dell\Drivers\CJDR8\Graphi...

Selected for restore: 0

Restore...

2. File Protection @ 6/7/2016 10:00 PM Found files: 10, directories: 0 (more available)

Restore...

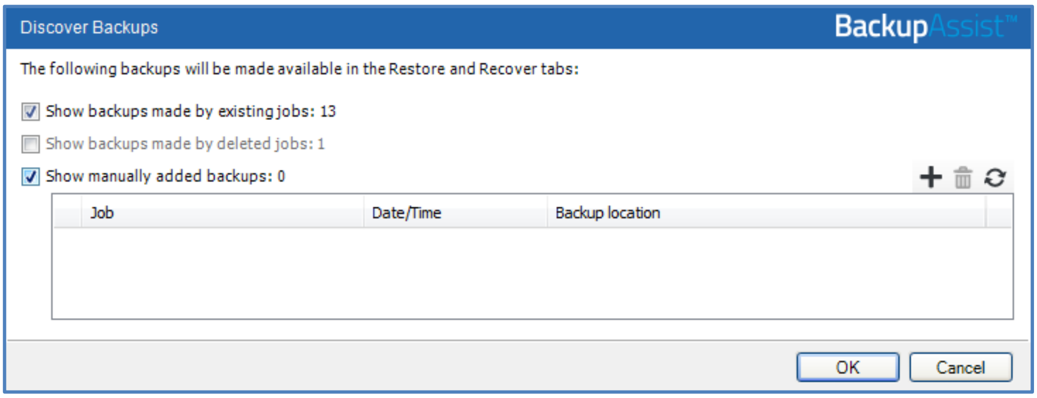
Figure 6: Restore Tab – Search page

a) The *Backups* section allows you to use the *Jobs* Filter, to limit the search to specific backup jobs. You can also use the *Backup Date* filter search within a specified date range.

b) The *Search* section is used to enter a search term associated with the name of the file you want to find. The *Search for* field will take the string provided and search for occurrences of that string within a file or directory name. The results of the search are displayed by backup.

   To refine the search, use the Created, Modified and Size options. Ticking any of these options will activate a drop down list of variables to select from. For Created and Modified, you can select a date using the Calendar selection fields. For Size, you can select the file size in bytes.

The **Discover Backups** button allows you to browse for backup catalogs created by deleted jobs and other servers. Selecting those backups will add them to the list of available backups.



The following backups will be made available in the Restore and Recover tabs:

☑ Show backups made by existing jobs: 13

□ Show backups made by deleted jobs: 1

☑ Show manually added backups: 0

Job	Date/Time	Backup location

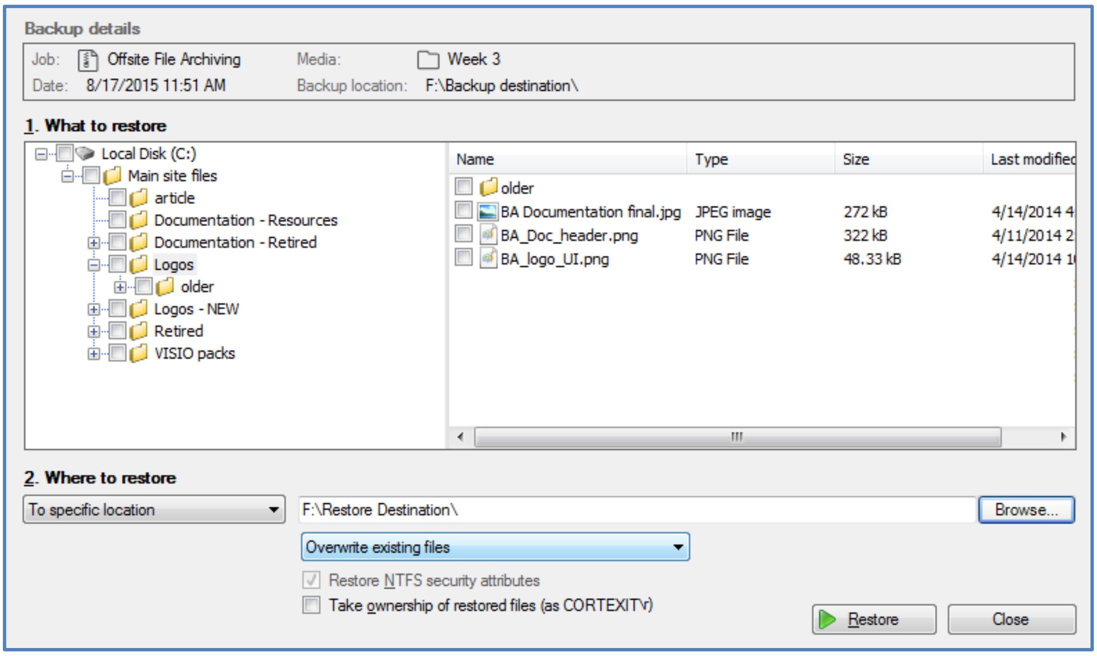
Figure 7: Discover Backups

3. **Select the backup that you want to restore from**

   Clicking on a backup's name will open the *Integrated Restore Console (IRC)*. The *Integrated Restore Console* is used to select the data to be restored, where to restore it to and the restore conditions.

4. **Select the files, folders or applications that you want to restore**

   - Use the left pane to locate and select the data that you want to restore.
   - The right pane will display the contents of the folder selected in the left pane.



Backup details

Job: Offsite File Archiving

Media: Week 3

Date: 8/17/2015 11:51 AM

Backup location: F:\Backup destination\

1. What to restore

- □ Local Disk (C:)
  - □ Main site files
    - □ article
    - □ Documentation - Resources
    - □ Documentation - Retired
    - □ Logos
      - □ older
    - □ Logos - NEW
    - □ Retired
    - □ VISIO packs

Name	Type	Size	Last modified
□ older			
□ BA Documentation final.jpg	JPEG image	272 kB	4/14/2014 4
□ BA_Doc_header.png	PNG File	322 kB	4/11/2014 2
□ BA_logo_UI.png	PNG File	48.33 kB	4/14/2014 1

2. Where to restore

To specific location

F:\Restore Destination\

Overwrite existing files

☑ Restore NTFS security attributes

□ Take ownership of restored files (as CORTEXIT\r)

Figure 8: Integrated Restore Console

5. **Select Where to restore the data to**

   Follow these steps to select the restore destination and restore options:

   a) Under *Where to restore* select *To original location* or *To Specific location*.

   b) Use the *Browse* button to locate and select the restore destination.

   c) Use the drop down box to set the overwrite rules. The overwrite rules will apply if the files being restored encounter files with the same name in the restore destination.

      You can select:

      - *Overwrite existing files* - The restored files will overwrite files in the restore destination.
      - *Do not overwrite existing files* – The restored files will not overwrite files in the restore destination. This means the files will not be restored.
      - *Only overwrite older files* - If a source file has changed since the backup was made it will not be overwritten.

   d) Review the *Restore NTFS security attributes* option

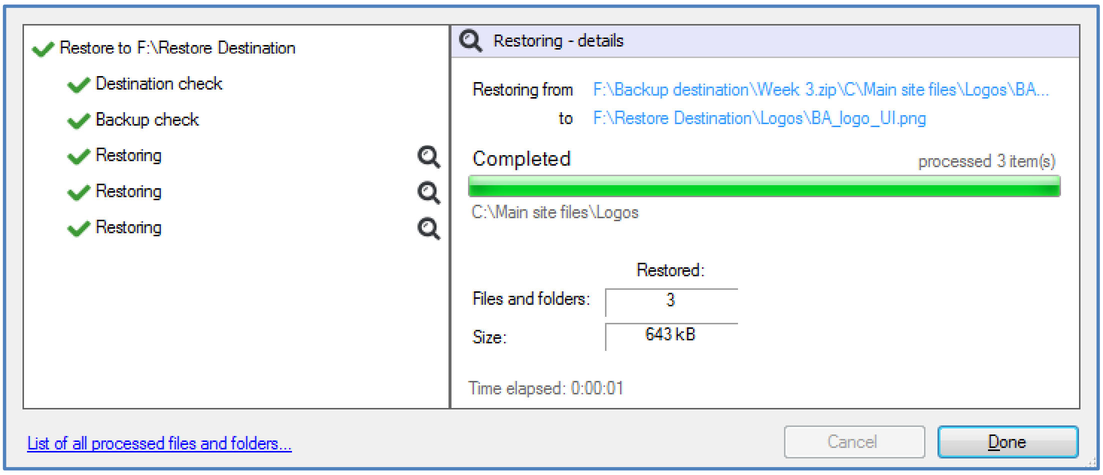
      If you select this option, the NTFS security attributes the file had when it was backed up will be retained when the file is restored. The NTFS security attributes can be viewed in the Security tab on the file's Properties

e) Review the *Take ownership of restored files* option

Selecting the *Take ownership of restored files* tick box will give the current user ownership of the restored files. The user is shown to the right of the text box description.

6. **Select Restore**

When you select the *Restore* button, the restore process will begin. The *Integrated Restore Console* will display information about the restore job and provide status updates as the job runs.



✓ Restore to F:\Restore Destination
- ✓ Destination check
- ✓ Backup check
- ✓ Restoring
- ✓ Restoring
- ✓ Restoring

Restoring - details

Restoring from F:\Backup destination\Week 3.zip\C\Main site files\Logos\BA...
to F:\Restore Destination\Logos\BA_logo_UI.png

Completed processed 3 item(s)

C:\Main site files\Logos

	Restored:
Files and folders:	3
Size:	643 kB

Time elapsed: 0:00:01

Figure 9: Integrated Restore console – restore monitor

Selecting *List all processed files and folders* ... will open notepad and display a list of the files restored, including their full path.

BitLocker Encrypted backups

If your backup is encrypted, you'll be prompted for the encryption password when the restore job tries to access the backup. 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.

If you encrypted the backup using BitLocker, you can use the password or encryption key to unlock the drive by connecting the flash drive. BackupAssist will use the key to unlock the drive that you are restoring from. You will not be prompted to do anything other than the normal restore steps.

7. **Select Done**

Once the restore has finished, selecting *Done* will return you to the main UI.

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

Helpful hint: 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 restoring 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 *Integrated 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.

7. 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 user guide

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.

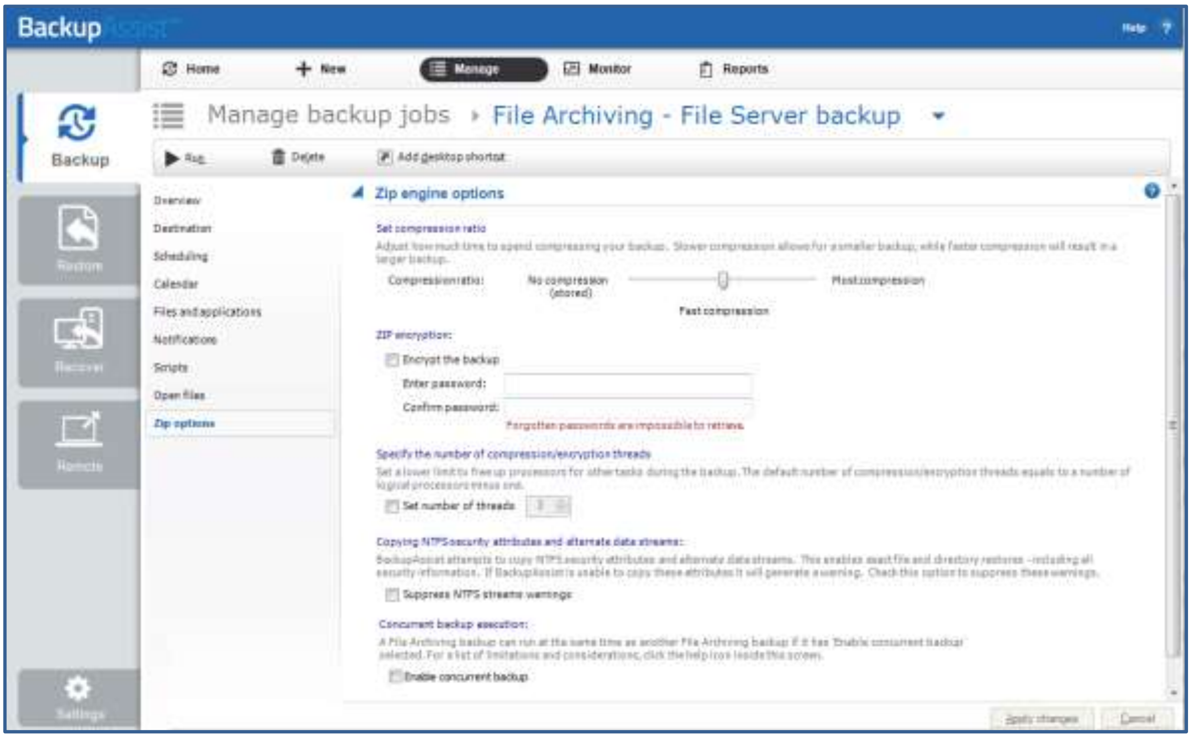
Customize schedule: This selection can be used to modify each backup within your current schedule. The default *Method* is a *Full* backup, but you can also select *Incremental*, *Differential* and *Copy*.

- **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 user guide

Zip options

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



Zip engine options

Set compression ratio

Adjust how much time to spend compressing your backup. Slower compression allows for a smaller backup, while faster compression will result in a larger backup.

Compression ratio: No compression (stored) — Most compression; Fast compression

ZIP encryption:

□ Encrypt the backup

Enter password:

Confirm password:

Forgotten passwords are impossible to retrieve.

Specify the number of compression/encryption threads

Set a lower limit to free up processors for other tasks during the backup. The default number of compression/encryption threads equals to a number of logical processors minus one.

□ Set number of threads 3

Copying NTFS security attributes and alternate data streams:

BackupAssist attempts to copy NTFS security attributes and alternate data streams. This enables exact file and directory restores - including all security information. If BackupAssist is unable to copy these attributes it will generate a warning. Check this option to suppress these warnings.

□ Suppress NTFS streams warnings

Concurrent backup execution:

A File Archiving backup can run at the same time as another File Archiving backup if it has 'Enable concurrent backup' selected. For a list of limitations and considerations, click the help icon inside this screen.

□ Enable concurrent backup

Figure 10: 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 Server 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 Server 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).