

BackupAssist™

BackupAssist v7

# File Protection Whitepaper

# Contents

<b>1. Introduction</b>	<b>2</b>
Documentation	2
Licensing	2
Modes of operation	2
Single-instance store	3
Advantages of File Protection over traditional file copy methods	3
<b>2. Backup considerations</b>	<b>4</b>
Exchange VM Detection	4
VSS Application backups	4
Restore vs. Recovery	4
Windows SystemState	5
<b>3. BackupAssist settings</b>	<b>6</b>
Backup user identity	6
Email server settings	6
Email address list	6
Network paths	6
<b>4. Creating a File Protection backup</b>	<b>7</b>
<b>5. Restoring from a File Protection backup</b>	<b>10</b>
<b>6. File Protection backup management</b>	<b>13</b>
Manually running a backup job	13
Destination: Enabling single-instance store	13
Scheduling	14
Files and applications	14
<b>7. File Protection backup report</b>	<b>15</b>
<b>8. Support and Resources</b>	<b>16</b>
Contacting Technical Support	16
Learn more – The Welcome Screen	16

# 1. Introduction

---



## File Protection

For historical versioning of files

Method: File Replication  
Backup to Disk / iSCSI / NAS / Rsync

BackupAssist File Protection is a feature for administrators who want a powerful, yet simple, file backup solution out-of-the-box. File Protection can be configured in minutes to create scheduled backup jobs without the need for complex scripts or settings.

File Protection backups replicate data to backup media and can take advantage of technologies such as *data encryption*, *backup-with-history replication* and *single-instance store*. File Protection can be used with other BackupAssist technologies, such as System Protection and RecoverAssist, for a complete data protection and data recovery solution.

## Documentation

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

- For information on backing up files over the internet see the [File Protection with Rsync Whitepaper](#)
- For information on the BackupAssist Backup tab, see the [BackupAssist Backup Tab Whitepaper](#).
- For information on the BackupAssist Restore tab, see the [BackupAssist Restore Tab Whitepaper](#).
- For information on the BackupAssist Recover tab, see the [BackupAssist Recover Tab Whitepaper](#).

## Licensing

File Protection is a standard feature included with the BackupAssist license. To back up data across the internet with Rsync requires the *Rsync 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](http://www.BackupAssist.com).

For instructions on how to activate / deactivate license keys, visit our [Licensing BackupAssist page](#).

## Modes of operation

File Protection offers two modes of operation: mirror and backup-with-history. For backups to removable media, the mode can be selected at the *Set up Destination* step when a backup job is created. For other media types, the mode is defined by the *schedule* selected in the *schedule* step.

### Mirror mode

The Mirror mode creates an exact replica of your files and folders (as the data appeared at the time of the backup). Only one backup will be stored at any one time, with no history available. This mode is useful for situations where a primary drive or a server needs to be replaced quickly.

### Backup-with-history mode

The *Backup-with-history* mode creates a new set of backup data in a uniquely named folder each time a backup job runs. Backups created using this mode are useful for maintaining version history over a long period of time. For backup jobs to disk-based destinations, you can even configure backup storage options to make sure that disk space on the backup destination is properly utilized.

## Single-instance store

BackupAssist's File Protection includes a powerful replication technology called single-instance store. With single-instance store enabled, only one unique copy of each file is stored on your backup device. Single-instance store backups are similar to incremental backups, because only new or modified files are actually copied to your backup device each time a backup runs. This saves time and disk space.

The single-instance store process is completely transparent. If no previous backup exists on the backup device, BackupAssist will perform a full backup of the selected data. For subsequent backups, only new or modified files will be backed up, but a new and complete backup set will appear on your backup device. This backup takes no more space than the new and modified files that were copied there.

If you view the backup destination, it will look as if a full backup was performed – refer to the backup report to confirm if a single-instance store is working correctly.

**Important:** File Protection backups cannot use single-instance store when the backup is saved on a ReFS formatted destination. This means all of the data will be backed up each time the backup job runs.

## Advantages of File Protection over traditional file copy methods

**No scripting required:** Easily set up basic mirroring backups for important files, or comprehensive archival backups with hundreds of days of backup history to restore from.

**Fully automated scheduling:** Backup jobs are automated with BackupAssist's one-click scheduler. The scheduler provides a selection of pre-configured, customizable backup schemes to choose from.

**Fully automated monitoring:** You will receive an automated email report after each backup job to inform you of the backup's success or failure.

**Multiple restore points:** Create a series of mirror backups on your backup device, one for each day. To restore, simply copy the files back to the relevant folder or use the BackupAssist Restore Console.

**Independent encryption:** Encryption (via TrueCrypt) can be set on the backup destination without affecting the data source.

**Volume Shadow Copy Service support:** BackupAssist is a VSS-aware application, so File Protection backups can detect VSS applications such as Exchange, SQL, Hyper-V and SharePoint.

**Preserve certain NTFS attributes:** A File Protection backup is able to preserve certain NTFS file attributes, set on the original source files. If you want to maintain NTFS file attributes we recommend you choose a backup destination formatted in NTFS. Preservation of NTFS attributes is enabled by default on destinations that support it.

File attributes at destination	Preserved?
Windows File Attributes	✓
Creation time	✓
Last modified time	✓
NTFS security (ACLs)	✓*
NTFS alternate data streams (ADSs)	✓*

\* Excludes Linux destinations

## 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

If your backup job contains a Hyper-V guest with an Exchange Server, the authentication information for that guest should be entered into the **Exchange VM Detection** tab on the **Selection** screen when you create the backup 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

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.

### VSS Application backups

The Volume Shadow Copy Service (VSS) is a Microsoft Windows Service that creates a copy of an application's data so the data can be backed up while the application is running. This means the data will not change or be locked while a backup is taking place. BackupAssist is VSS-aware, so File Protection, File Archiving and System Protection backups can detect VSS applications such as Exchange, SQL, Hyper-V and SharePoint. BackupAssist will display a VSS application as an application container during the *Destination* step of the backup job's creation. You can select the container or individual components and BackupAssist will select the files that need to be backed up.

In some cases, only applications that are running will be detected. If an application is not listed, try restarting the application and the VSS service and then click the *Refresh* button in BackupAssist.

For Windows Small Business Server 2003, a registry entry modification is needed to see an Exchange Server. See our online blog post, [Backing up Exchange with SBS 2003](#), for more information.

### 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](#).

## Windows SystemState

### Overview

In previous versions of BackupAssist, Windows SystemState was called System State and it was available during the creation of a backup job. The Windows SystemState option is now selected by editing a backup job after it has been created. There are exceptions, as shown in the table below.

A Windows SystemState backup contains some of the important files, registry values and settings that are used by the Windows operating system. It does NOT back up the operating system itself. This means a Windows SystemState backup can be used to restore the settings your computer had at an earlier point in time, but it will not allow you to recover your computer. A Windows SystemState backup can be helpful if your computer is encountering errors and you want to restore your settings to an earlier point in time, before the errors occurred.

Because Windows SystemState requires a functioning computer, and can only *restore* Windows settings, we recommend that a bare-metal backup is used. A bare-metal backup can restore Windows SystemState data, and it can ALSO be used to perform a *recovery* of your computer, when used with a Windows recovery environment, like RecoverAssist.

### Selecting Windows SystemState

Windows SystemState can be selected after a backup job has been created, if you have enabled the *Windows settings*. The exceptions, considerations and steps required are explained below:

This table shows what backup jobs can include Windows SystemState.

	NTBackup (Windows 2003)	File Archiving, File Protection and System Protection backup jobs	File Archiving zip-to-tape backup jobs	File Protection Rsync backup jobs
During the creation of a new backup job	YES	NO	NO	NO
By editing an existing backup job	YES	YES, if enabled	YES	NO

#### To enable Windows SystemState:

1. Select the BackupAssist *Settings tab*.
  2. Select *Windows settings*.
  3. Tick *Enable v6 compatible Windows SystemState selection*.
- ❖ Backup jobs created in earlier versions of BackupAssist (that included System State) will have the setting enabled by default in BackupAssist v7.
  - ❖ Zip-to-tape backup jobs will not need to enable this setting, to select Windows SystemState.

#### To select Windows SystemState:

1. Select the BackupAssist *Backup tab*, and then select the *Manage* menu.
2. Select the *backup job* that you want to modify, and then select *Edit* from the menu.
3. Select *Files and applications* from the left pane.
4. Select *Windows SystemState* at the top of the data selection pane.

## 3. 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.

## 4. Creating a File Protection backup



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

Launch BackupAssist and follow the steps outlined below:

1. Select the **Backup** tab, and click **Create a new backup Job**
2. Select **File Protection**

If this is the first time you have created a backup job, you will be asked to provide a *Backup user identity* if one has not been defined. 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.

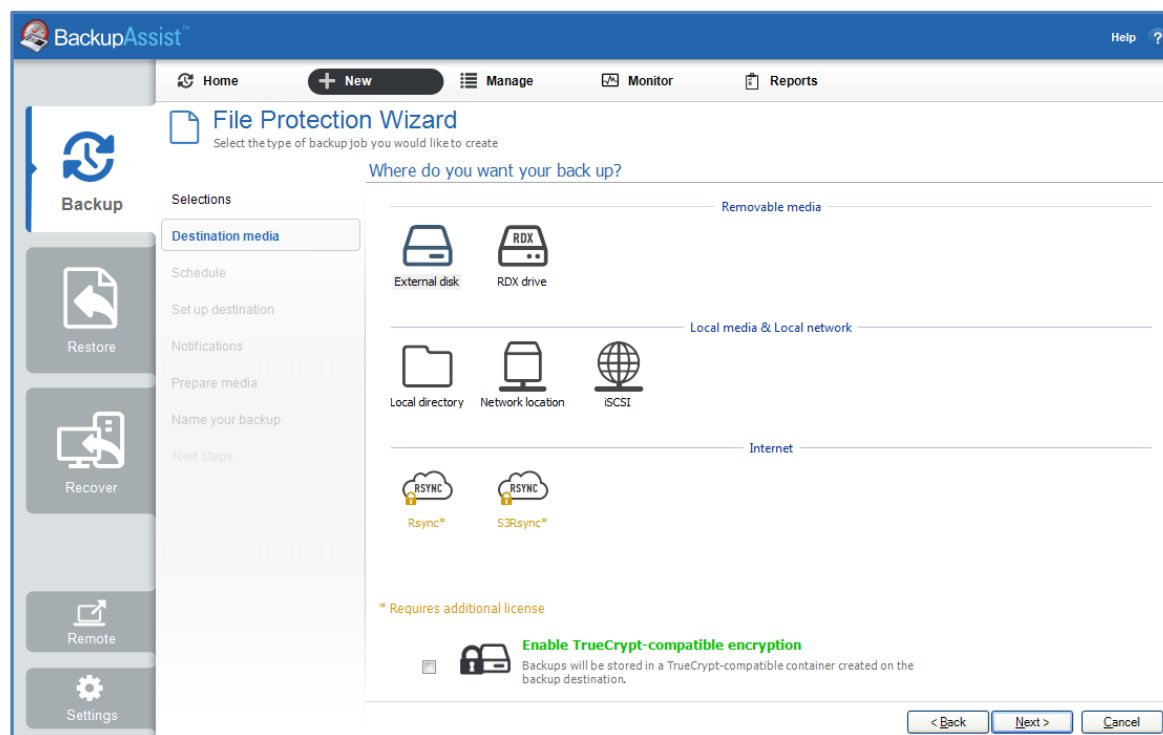
Select the volumes, folders, files and applications that you want to back up, and click **Next**.

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.

Select a device for your backup destination, and click **Next**.

To back up to an Rsync destination, refer to the [File Protection using Rsync Whitepaper](#).

Select **Enable TrueCrypt** if you want the backup to be encrypted. The first time you use this feature, TrueCrypt will install the encryption files.



**Figure 1: File Protection backup – Destination media selection screen**



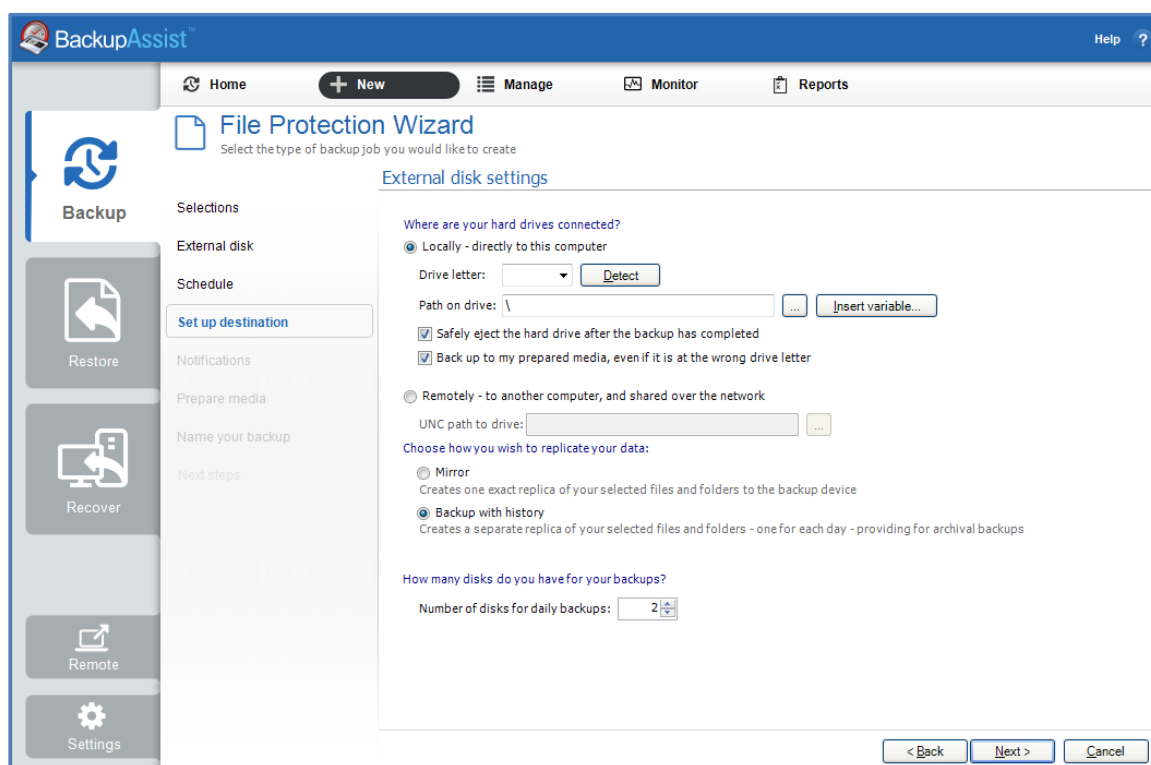
5. **Schedule:** This screen is used to select when and how you would like the backup job to run, and how long you would like the backup to be retained for. A selection of pre-configured schedules, called schemes, will be displayed.

- 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 schedule can be customized after the backup job has been created.

Select an appropriate scheme, and click **Next**.

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.

Configure your backup destination, and click **Next**.



**Figure 2: BackupAssist File Protection – Set up destination screen**

- If your media is removable, you can set the media to eject after the backup job has finished.
- If your media is a removable drive, you can select either *Mirror* or *Backup-with-history* for the replication mode. For non-removable media, the mode is determined by the scheme in step 5.
- If you selected *TrueCrypt* for data encryption, you will be prompted to create a password.

**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.

➤ **Mail Server:** If you have not configured an SMTP mail server for BackupAssist, you will be prompted to provide those details after the backup destination step has been completed. See the [BackupAssist settings](#) section for guidance.

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 [BackupAssist Backup tab whitepaper](#).

8. **Prepare media:** If you selected a portable media device as your backup destination (such as an external HDD or a RDX drive) 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 are 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:

- d. Enter the name and drive designation to be used for each media device listed.
- e. Select **Prepare** for each media device listed.

BackupAssist will now write the label to the media so that it is able 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 labeled Wednesday, BackupAssist will warn you that the incorrect media has been detected.

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

► **Your File Protection 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 Protection backup management](#), for more information.

**Important:** Once a backup job has been run and a backup created, a MANUAL test restore should be performed to ensure the backup is working as intended. To perform a test restore, refer to the section, [Restoring from a File Protection backup](#).

## 5. Restoring from a File Protection backup



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

To restore data from a **File Protection** 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. When you select one of the restore categories provided, BackupAssist will locate the corresponding backups for you.

- *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 backups catalogued by BackupAssist that match your selection. The backups will be grouped by the backup's source location, and by 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**.

The screenshot shows the BackupAssist interface with the 'Restore' tab selected. The 'Files & Folders' category is chosen, displaying a list of backup jobs grouped by source location. Each group has a 'Restore Console' button.

Job	Backups	Earliest	Latests
<b>Files on recovery</b> 1 backup(s)			
<b>Files on work</b> 13 backup(s)			
Archive to Tape	13	22/01/2013	7/02/2013
<b>Files on C:</b> 41 backup(s)			
Daily Backup - Main office	3	11/02/2013	13/02/2013
SQL File Archiving	3	8/02/2013	12/02/2013
File Archiving - Local Directory	4	30/11/2012	11/02/2013
SQL File Protection	1	8/02/2013	8/02/2013

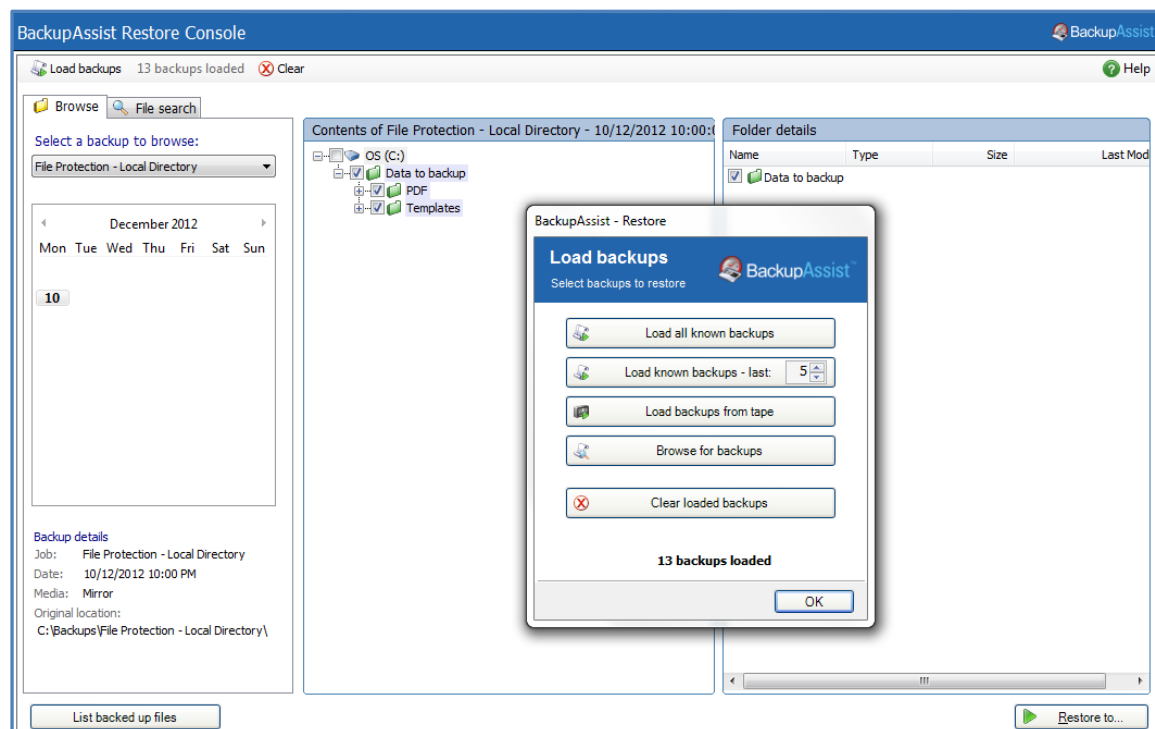
**Figure 3: BackupAssist Restore Home page – selection results**

#### 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.



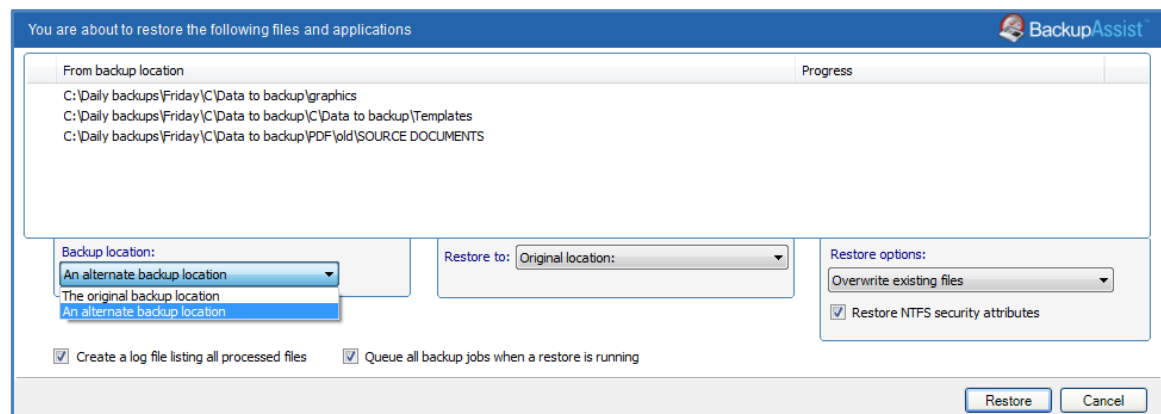
**Figure 4: BackupAssist Restore Console – backup and data selection**

If the backup is not present, or if you wish to load additional backups, select the **Load backups** option. Click **Load all known backups** to load all backup catalogues.

For more information about data selection, refer to the [Restore tab whitepaper](#).

## 5. Restore Console – restore destination selection

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



**Figure 5: 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.  
See the [File Protection Advantages](#) section for information on NTFS attributes.
- 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 Protection restore has now been completed.

**Important:** Only backups made with BackupAssist v5.3 or later will show up in the Restore Console.

**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 Protection* backup, you can browse to the location of your backup using Windows Explorer and copy the required files to any location.

## 6. File Protection 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.

### 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.

### Destination: Enabling single-instance store

*Removable media backups* created with the *Backup-with-history* mode selected can be configured to use *single-instance store*, so that only one unique copy of each file is stored on the backup destination. Single-instance store is enabled by default. Backups cannot use single-instance store when the backup is saved on a ReFS formatted destination (e.g. Windows Server 2012).

To modify this setting:

- a. Select **Destination** from the left menu and expand **Replication Mode Options**.
- b. Check the option, **Use the single-instance store**.

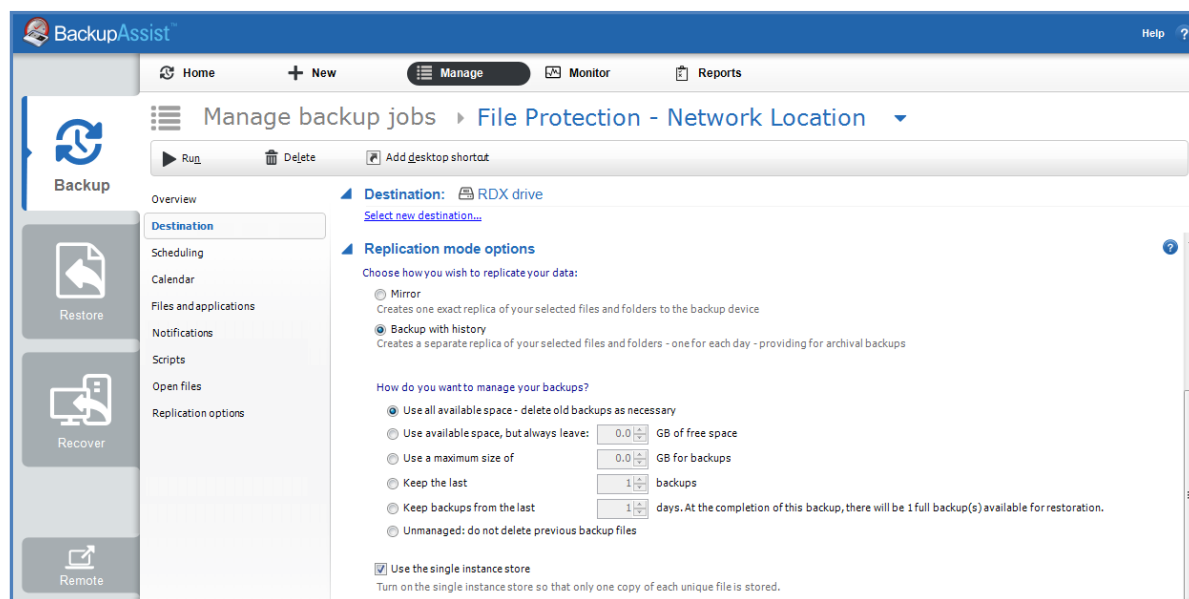


Figure 6: Manage backup – Removable media, destination screen

## 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 customizations available will depend on the type of backup media used. For File Protection backups, the *Method* field can only be set to *Automatic*. This is because single-instance store provides the benefit of incremental backups in a full backup format. This technology is managed by BackupAssist and does not require further modification.

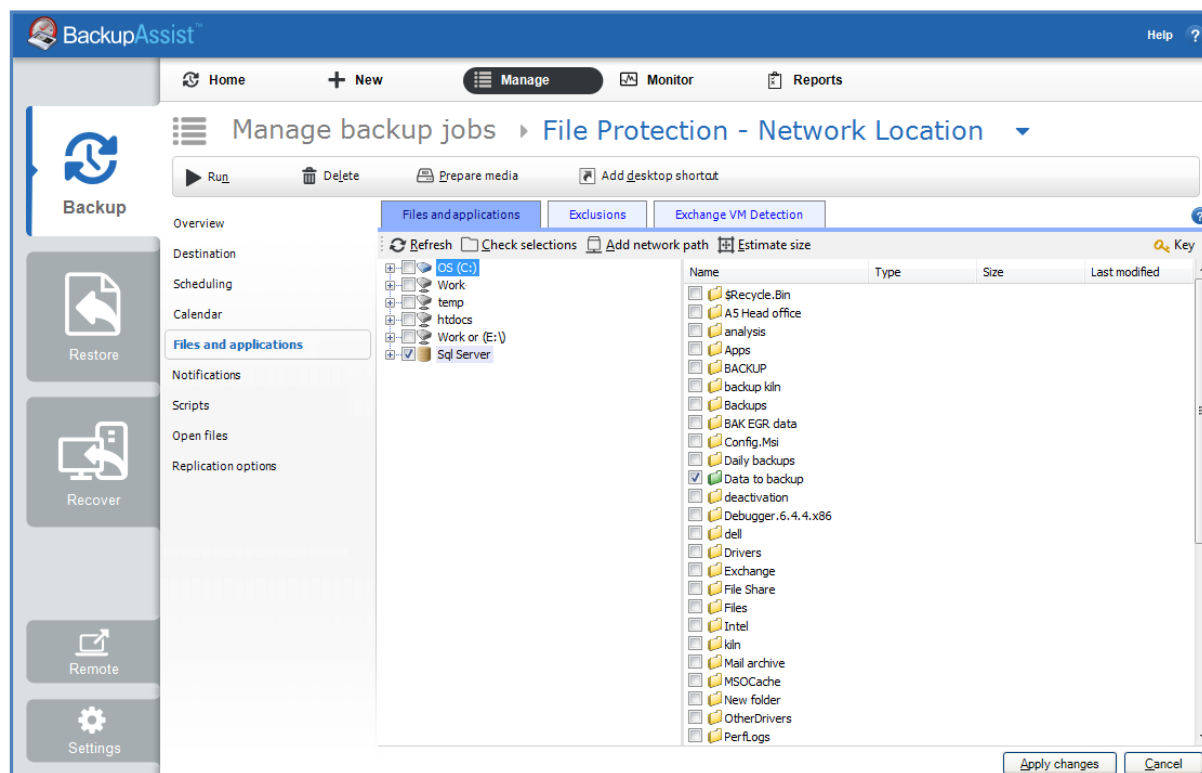
For additional information on the *Scheduling* screen, please refer to the [Backup tab whitepaper](#).

## Files and applications

If your backup job contains a Hyper-V guest with an Exchange Server, the authentication information for the guest should be entered into the **Exchange VM Detection** tab. Select the **File and applications** > **Exchange VM Detection** tab.

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

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.



**Figure 7: Manage backup jobs screen – File and applications option**

## 7. File Protection backup report

BackupAssist File Protection reports are very similar to those created from other backup engines. Some sections, however, are unique to File Protection and explained in greater detail below.

The **File Replication** section of the backup report, outlines how much data was backed up, how many files were backed up and includes details about single-instance store (if enabled).

The details outlined in the File Replication section include:

- **Total file count:** The total number of files that were selected for backup.
- **Files copied:** The actual number of files copied during the backup. If no files have been modified or no new files have been added since the last backup, BackupAssist will not copy them to your backup destination.
- **Files where no copy required:** If single-instance store is enabled, files that have not been changed since the last successful backup do not need to be copied to your backup destination.
- **Total size:** The total size of a full backup (i.e. all files selected for backup).
- **Size of files copied:** The amount of data that actually needed to be copied for this backup (i.e. new or modified data not already present at the backup destination).
- **Size of files where no copy required:** The total size of the files that did not need to be backed up due to single-instance store.

The **Media Usage** section of the backup report provides a list of File Protection backups stored at the backup's destination. This list can help you determine the number of backups stored on a device that you can restore from, and monitor the amount of free space available.

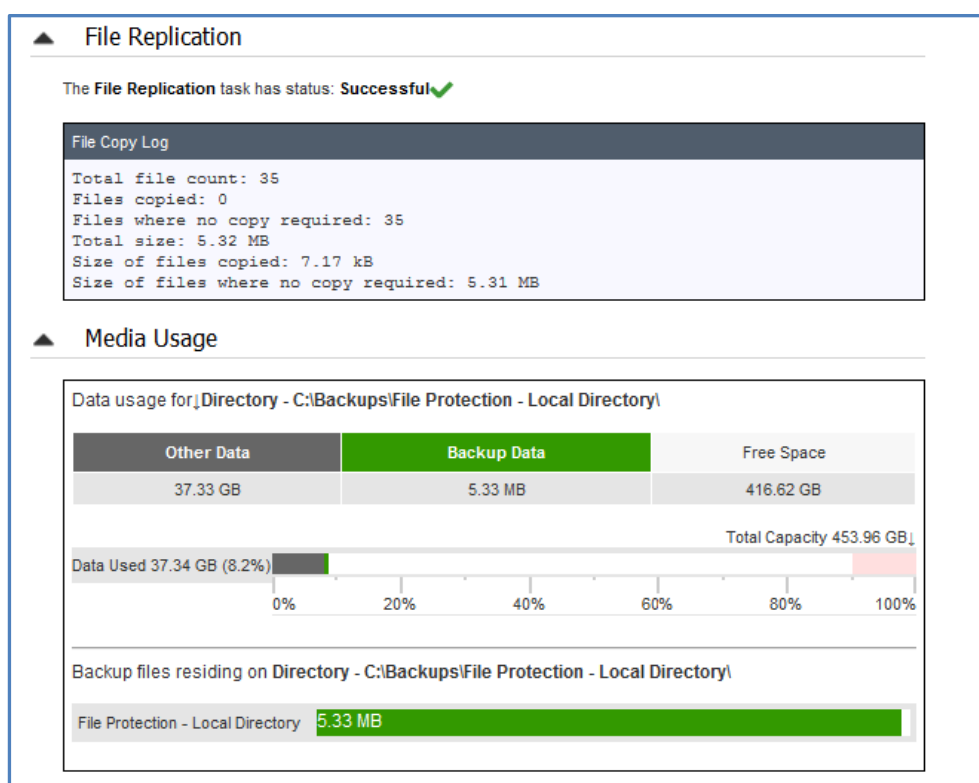


Figure 8: File Protection backup report



## 8. Support and Resources

### Contacting Technical Support

Should you have any questions regarding either BackupAssist or File Protection, please email [support@backupassist.com](mailto:support@backupassist.com) and we will respond to you as soon as possible.

Similarly, if you have any suggestions for additional functionality in BackupAssist, or new products or add-ons, please also forward your feedback to [support@backupassist.com](mailto:support@backupassist.com)

### Learn more – The Welcome Screen

Each tab in BackupAssist includes a “Learn More” link on the tab’s **Home** page.

For example, selecting the **Learn more about Backup** link will open the **Welcome Screen** with the Backup introduction selected. This screen provides an overview of the tab’s functions and features, and links to documentation and resources.

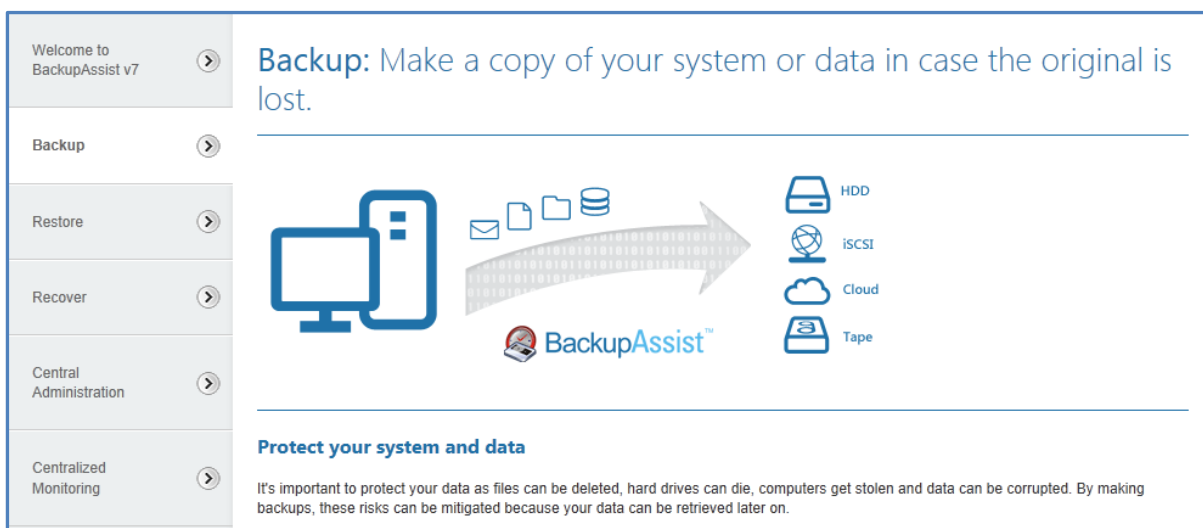


Figure 9: Backup tab – Welcome Screen