BackupAssist™ v8

File Protection

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 Protection is a fully-featured solution for those 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.

Documentation

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

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

Other BackupAssist documentation can be accessed through the Documentation webpage

- 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 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.

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

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.

BackupAssist Settings

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 using the *Backup user identity* option on the *Settings* tab, and your backup jobs will be launched using these credentials.

Email server Settings

An SMTP server must be configured if you want to have the email *Notifications* step enabled when you create a backup job. Use the *Mail Server* option on the *Settings* tab to enter the server's details.

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 support

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.

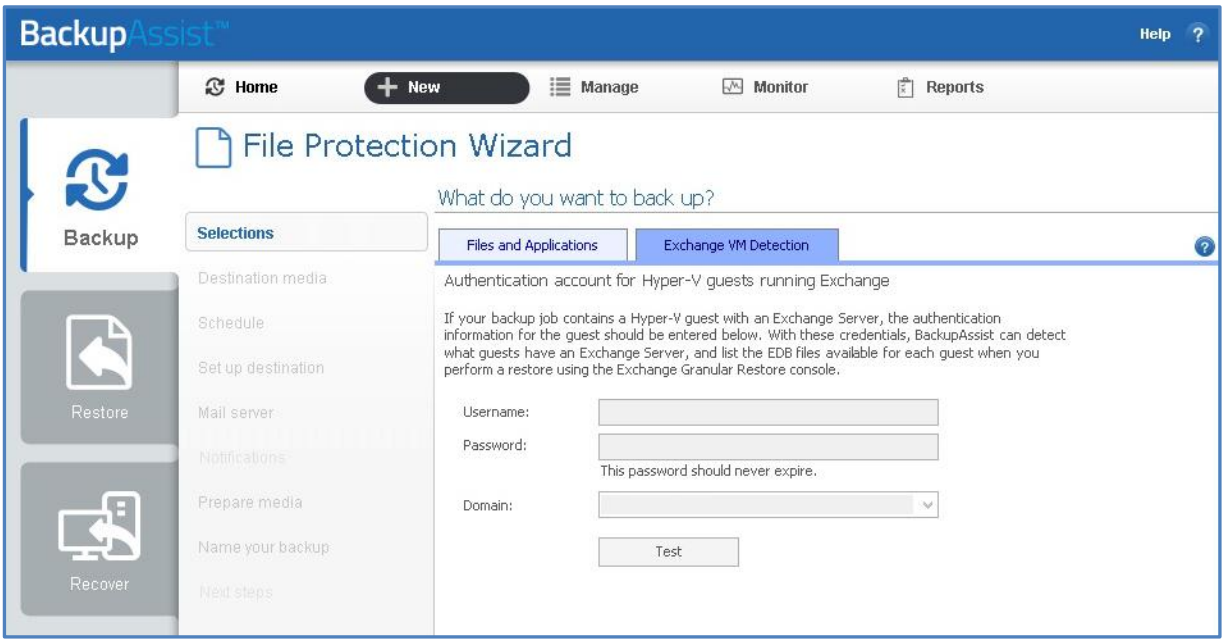

Figure 1: Selection screen - for an Exchange Server on a Hyper-V guest

The Exchange VM Detection tab appears when the Hyper-V role is installed and running on the server. If you back up multiple 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 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*. 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.
      - TrueCrypt encryption is available for all destinations. The first time you use this feature, TrueCrypt will install the encryption files.
      - 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.**

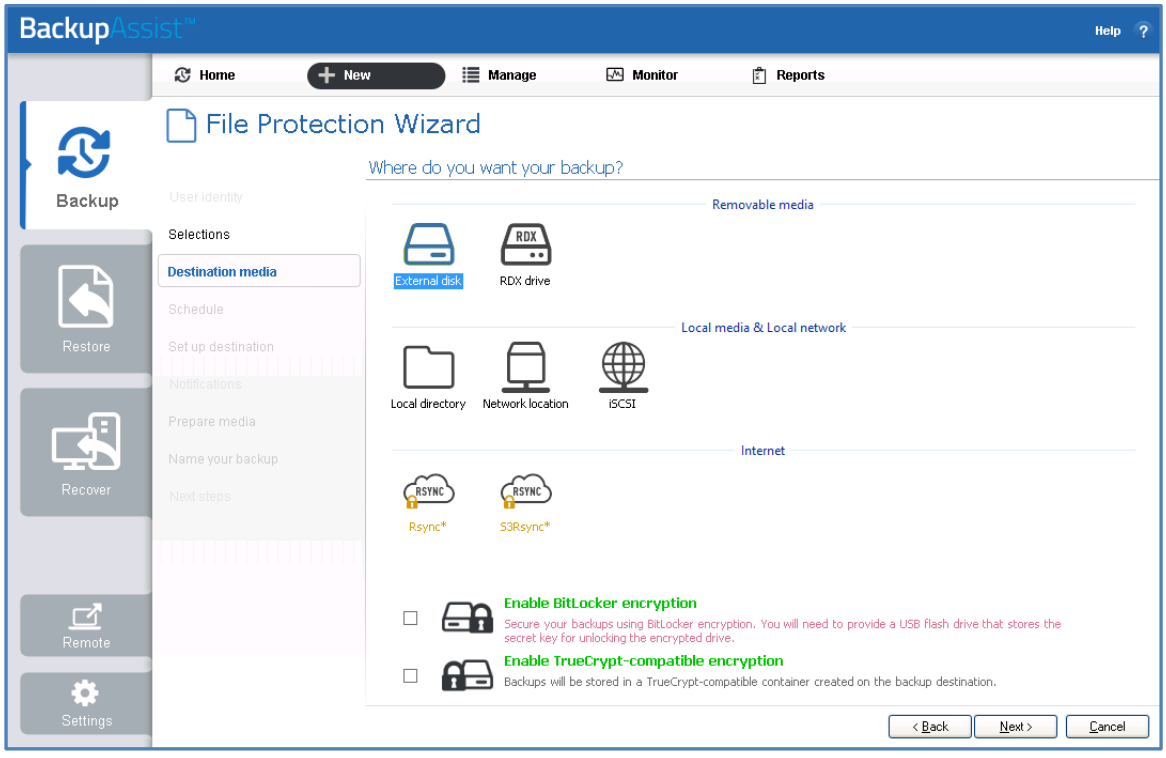

Figure 2: File Protection backup – Destination media selection screen

To back up to an Rsync destination, refer to the File Protection using Rsync guide.

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 an appropriate 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.

To learn more about File Protection schedules, refer to the Backup management section below.
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.

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

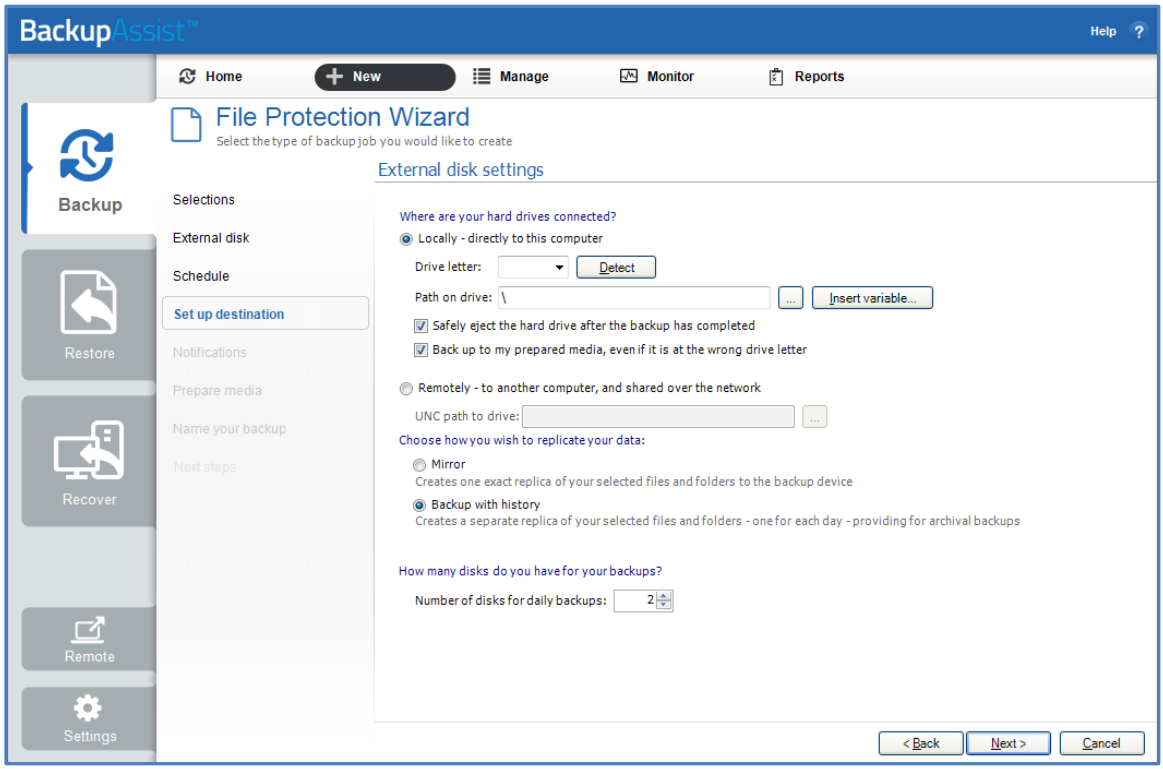

Figure 3: BackupAssist File Protection – Set up destination screen

- 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* 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.

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

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 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:

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

   b. Select **Prepare** for each media device listed.

   BackupAssist will write the label to the media so it can recognize the media and ensure that it is 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.

   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**.

▶ **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 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.

Please note that 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 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.

   - *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.**

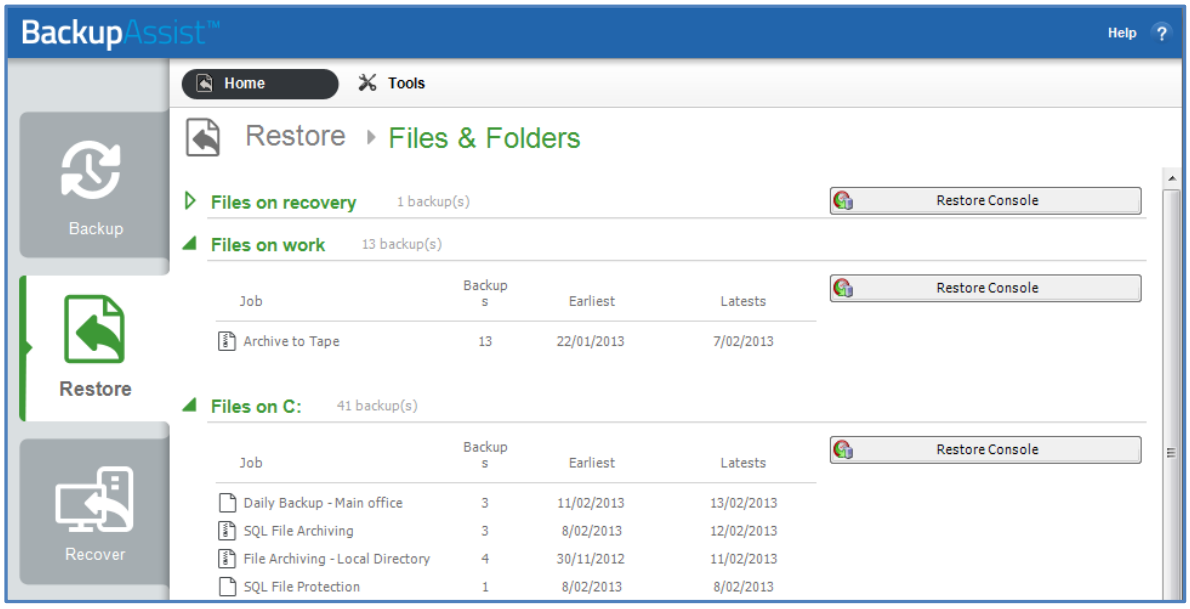

Figure 4: BackupAssist Restore Home page – selection results

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.

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*.

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*.

   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 (doesn't recreate 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 Protection 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.

5. 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**.

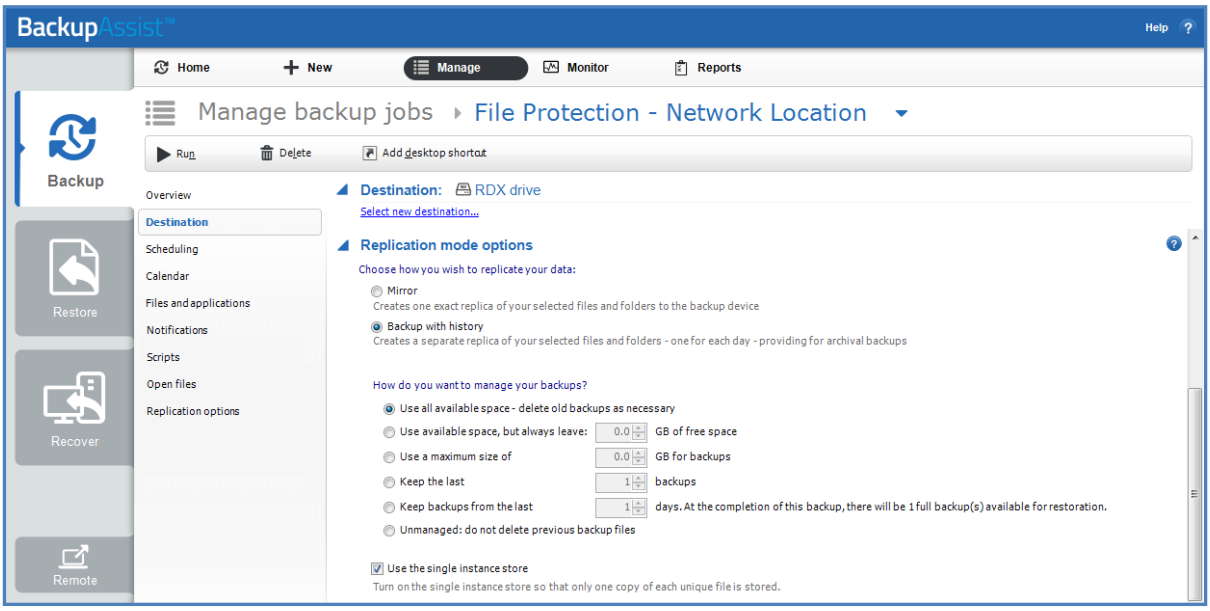

Figure 5: Manage backup – Removable media, destination screen

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.

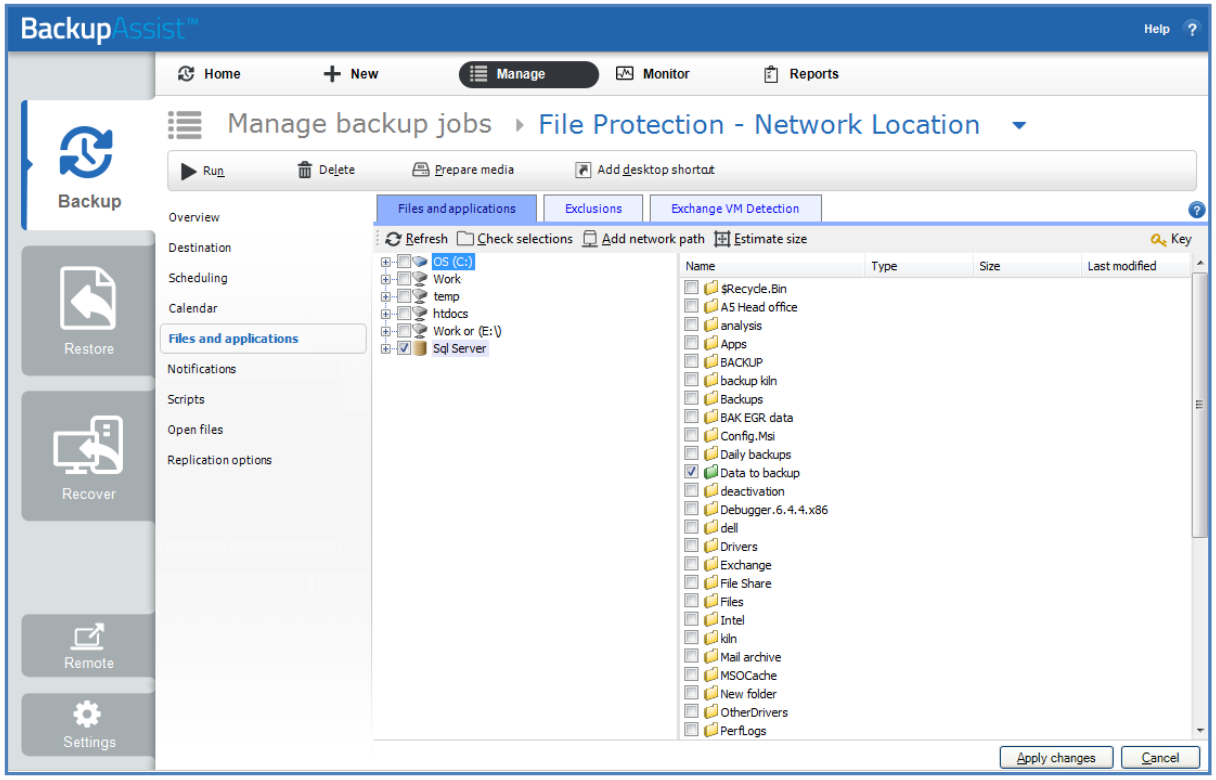

Figure 6: Manage backup jobs screen – File and applications option