BackupAssist™v9

# File Protection

## User guide

backupassist.com

Cortex I.T.

# Contents

# 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 user guide 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 user guide
- 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 the Settings Recover tab, see the 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 *Offsite Backups 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.

## 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

This section looks at the advantages of File Protection over traditional file replication 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 Integrated Restore Console.

**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) | ✓* |

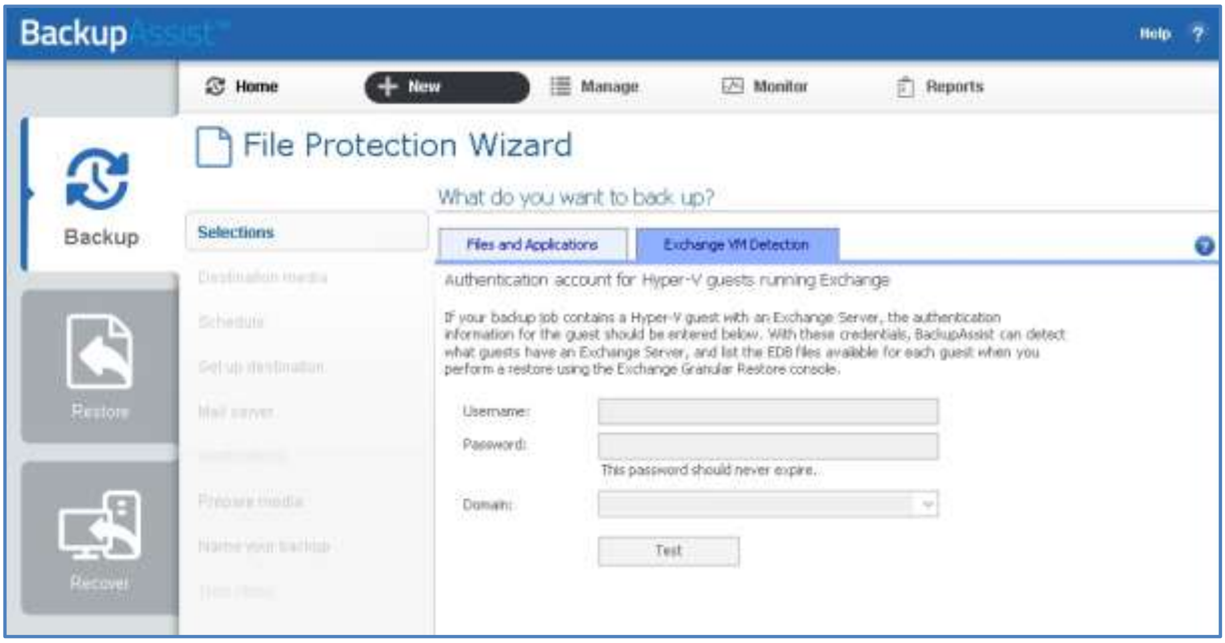
* Excludes Linux destinations

# 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 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.



File Protection Wizard

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 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 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

# 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*. See the section above, BackupAssist settings, for guidance.

3. **Selections**

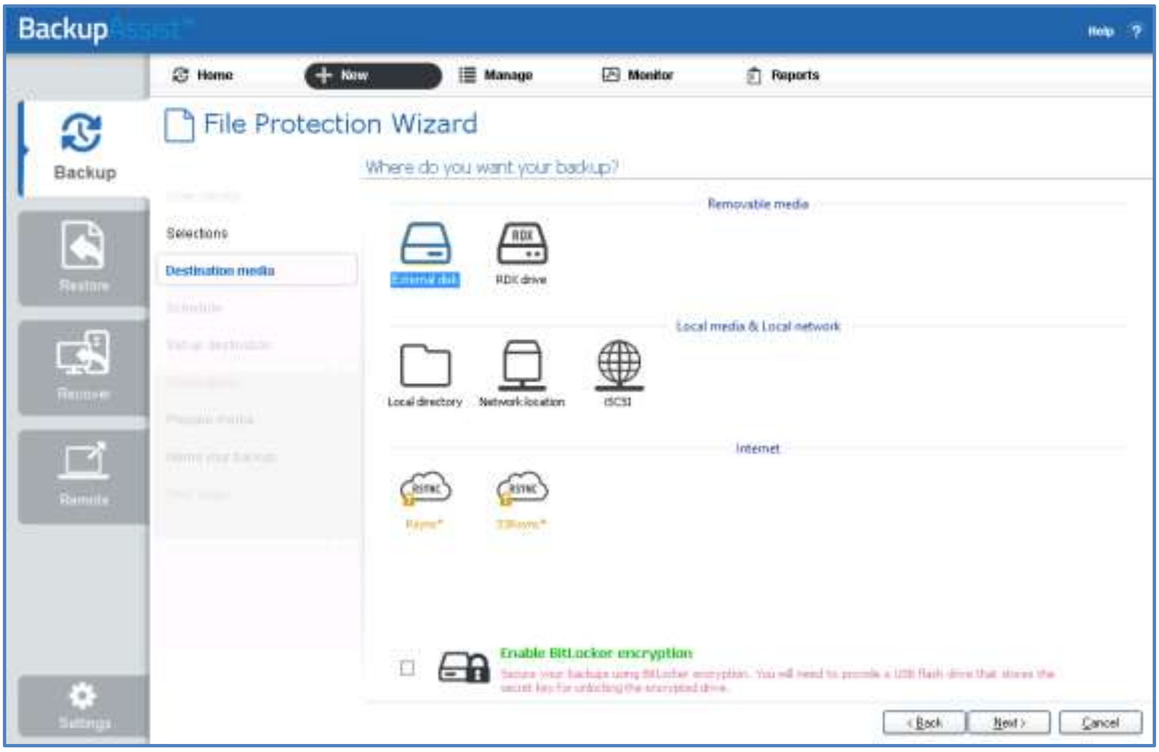
   The selections screen is used to select the data and applications that you would like to back up. Any VSS applications detected will be displayed here as application directory containers.

   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.



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.

**Figure 2: File Protection 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.

BitLocker encryption is available on Windows Server with External disk or RDX drive destinations. BitLocker will encrypt the destination media. To learn more, see our BitLocker resource page.

c. Click **Next.**

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.

- 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.

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

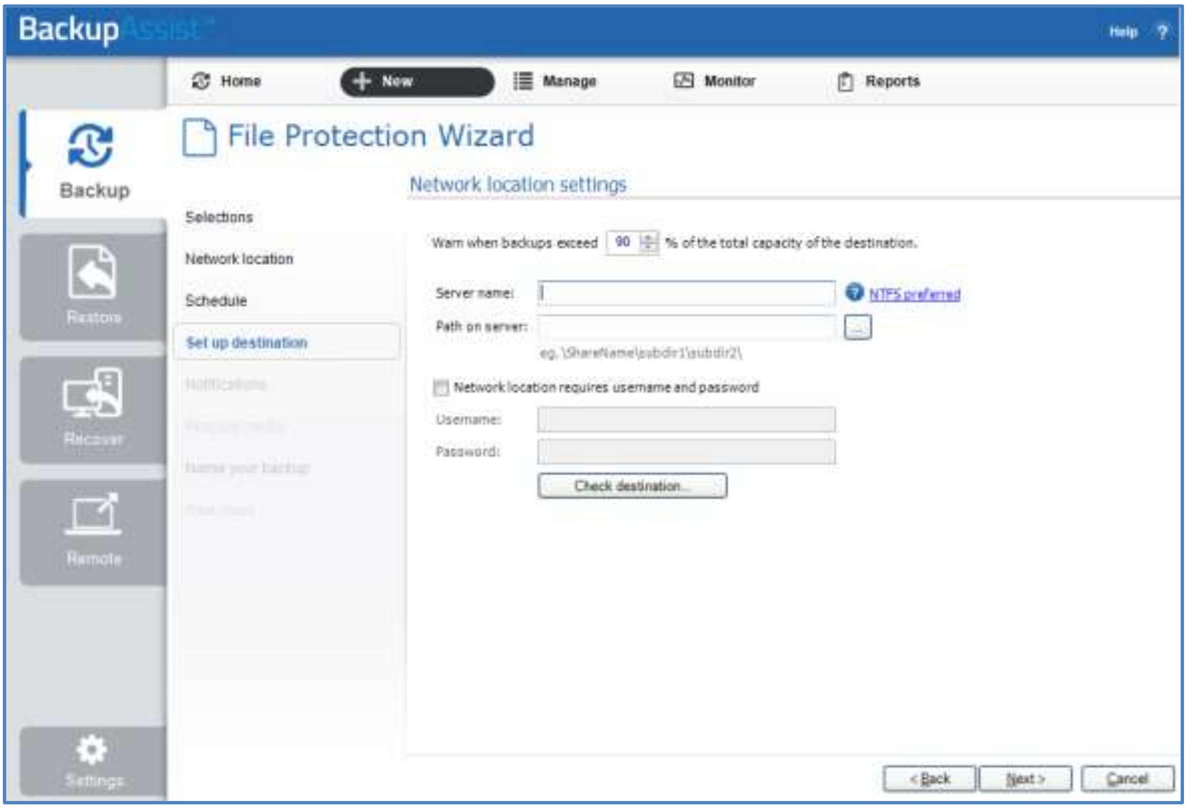
For detailed information on scheduling options and customizations, see the Backup tab user guide.

### 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.

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.



Network location settings

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

Server name: NTFS preferred

Path on server: eg. \ShareName\subdir1\subdir2\

□ Network location requires username and password

Username:

Password:

Check destination...

**Figure 3: BackupAssist File Protection – Set up destination screen**

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

- 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.

> **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 BackupAssist settings section to learn more or the Backup tab user guide for instructions.

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.

### 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*.

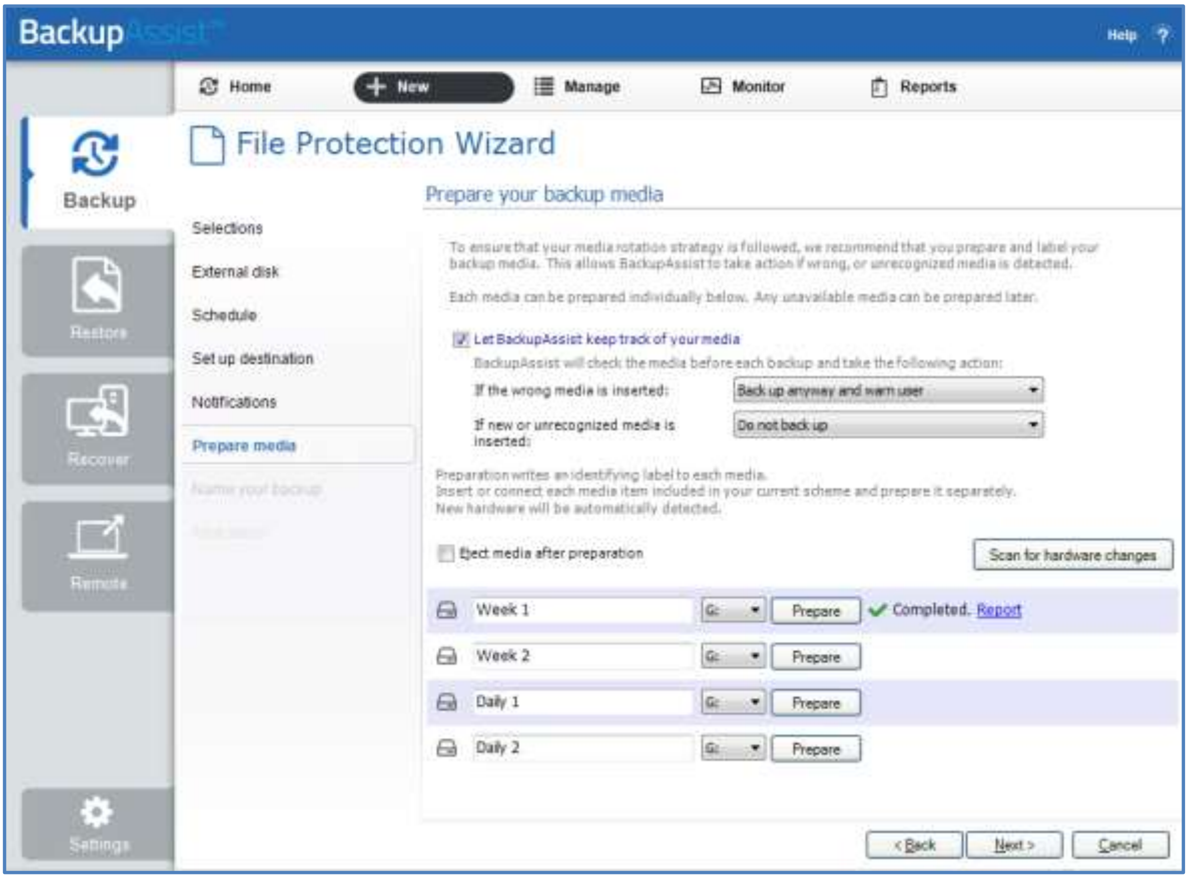
BackupAssist will display all removable media that are currently attached, along with a text field and drive designation drop-down box, which can be used to provide a label for the media.

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.

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.



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

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

**Figure 4: BackupAssist File Protection – Prepare media screen**

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.

# 5. Restoring from a File Protection 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 Protection** backup, follow these steps:

1. **Select the Restore tab**

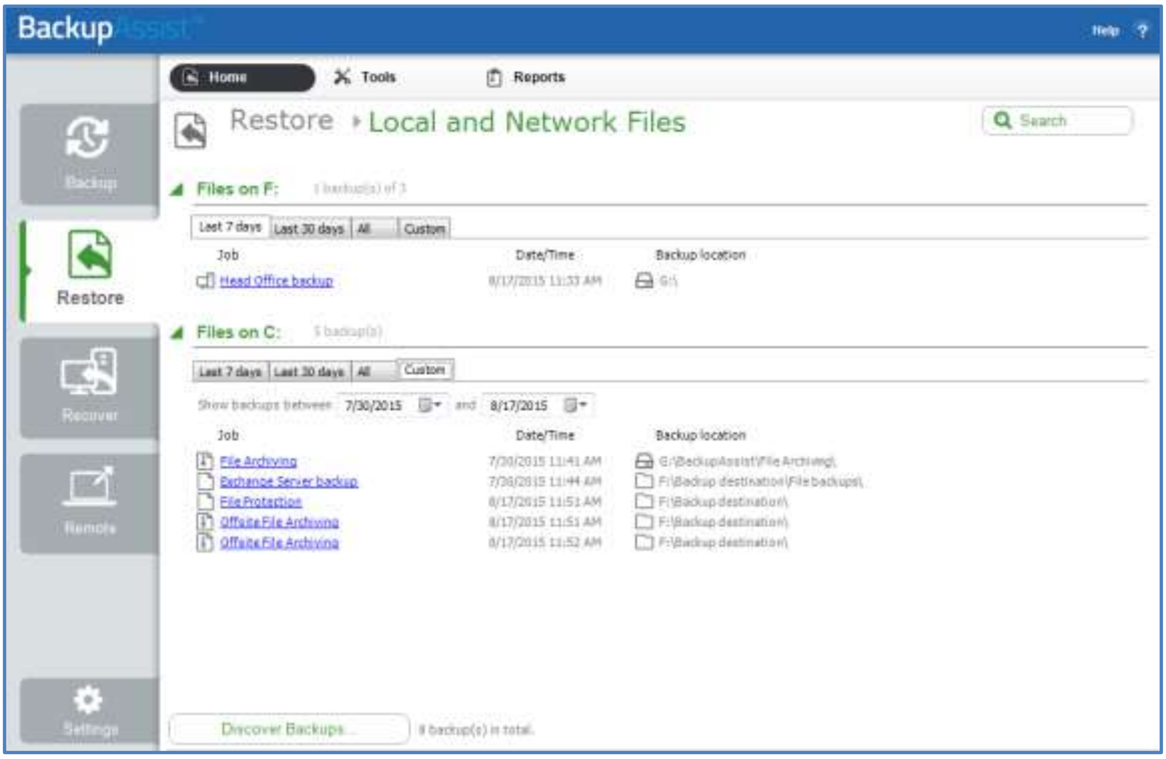
   The *Restore tab* has a *Home page* and a *Tools page*. The *Home page* is the default page and the recommended starting point for performing a restore. The *Tools page* should only be used by experienced administrators or users being assisted by technical support.

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, which is explained below.

   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

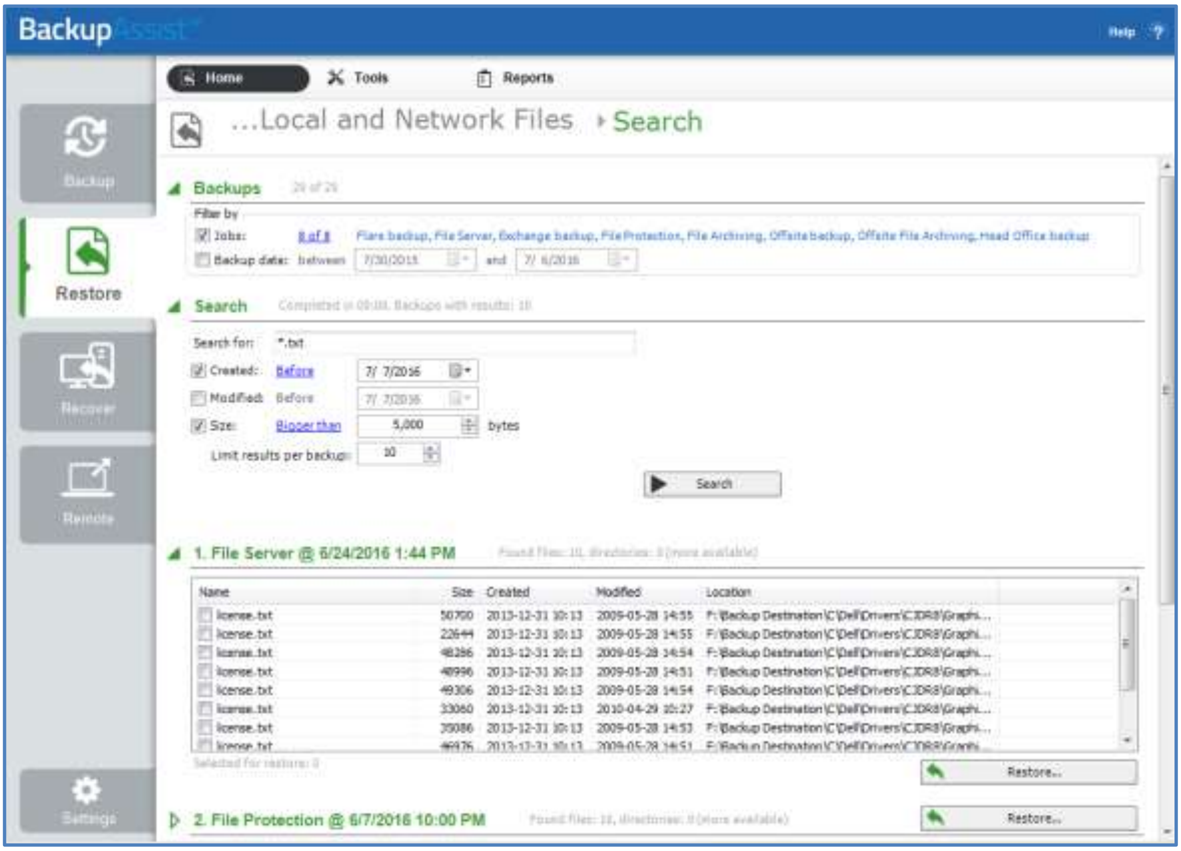
Show backups between 7/30/2015 and 8/17/2015

| 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…

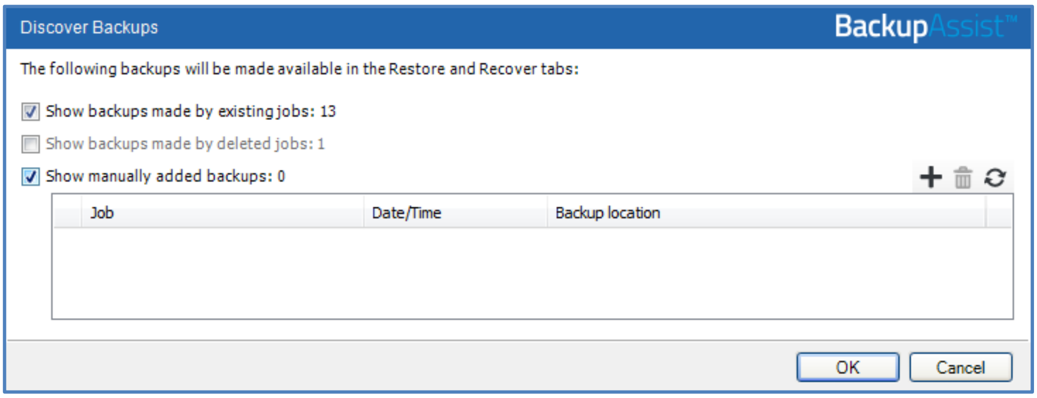
**Figure 6: Restore Tab – Search page**

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.



Discover 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 |
|---|---|---|

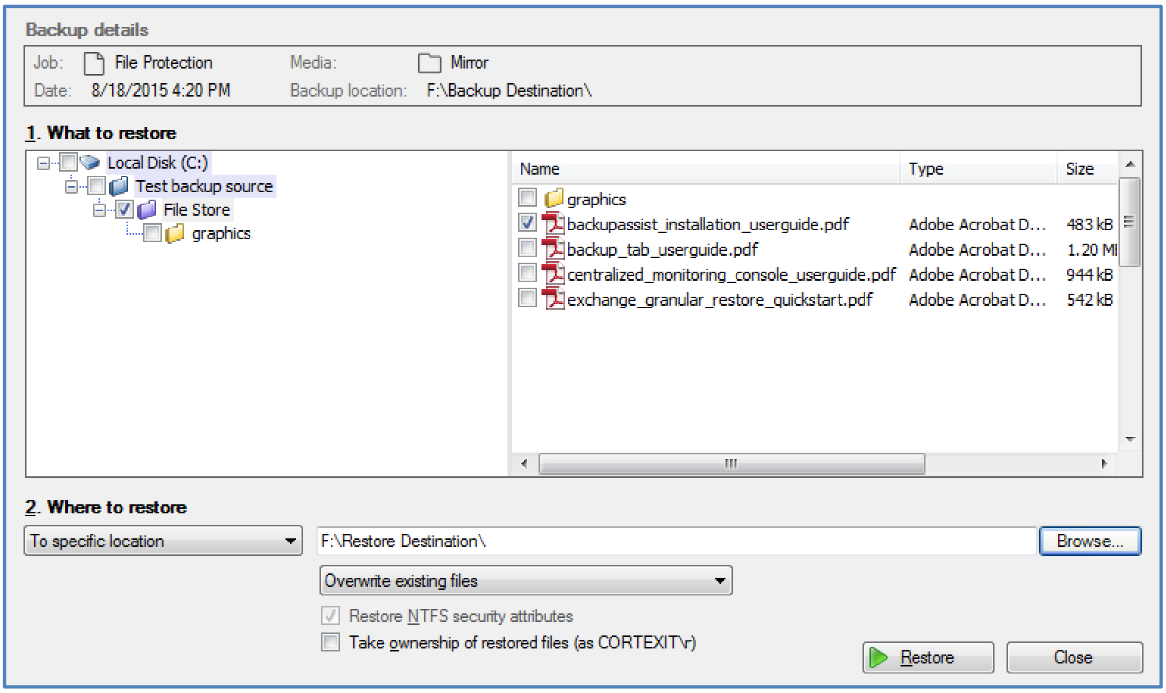
**Figure 7: Discover Backups**

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: File Protection    Media: Mirror

Date: 8/18/2015 4:20 PM    Backup location: F:\Backup Destination\

1. What to restore

- □ Local Disk (C:)
  - □ Test backup source
    - ☑ File Store
      - □ graphics

| | Name | Type | Size |
|---|---|---|---|
| □ | graphics | | |
| ☑ | backupassist_installation_userguide.pdf | Adobe Acrobat D... | 483 kB |
| □ | backup_tab_userguide.pdf | Adobe Acrobat D... | 1.20 MI |
| □ | centralized_monitoring_console_userguide.pdf | Adobe Acrobat D... | 944 kB |
| □ | exchange_granular_restore_quickstart.pdf | Adobe Acrobat D... | 542 kB |

2. Where to restore

To specific location    F:\Restore Destination\    Browse...

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

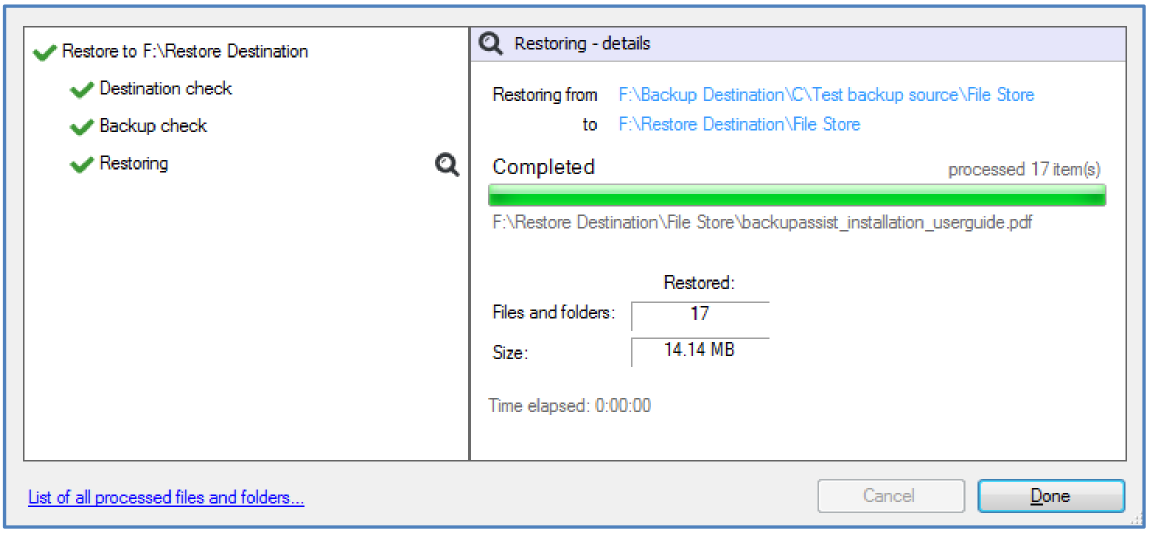
If you select this option, the NTFS security attributes the file had when it was backed up will be retained when the file is restored. The NTFS security attributes can be viewed in the Security tab on the file's Properties

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 - details

Restoring from F:\Backup Destination\C\Test backup source\File Store
to F:\Restore Destination\File Store

Completed processed 17 item(s)

F:\Restore Destination\File Store\backupassist_installation_userguide.pdf

| | Restored: |
|---|---|
| Files and folders: | 17 |
| Size: | 14.14 MB |

Time elapsed: 0:00:00

**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.

**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 Protection restore has now been completed**

**Helpful hint:** 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, as long as the files are not encrypted.

# 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** and **Manage** from the top menu.
2. Select the backup job you want to modify, and select **Edit.**
3. 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.

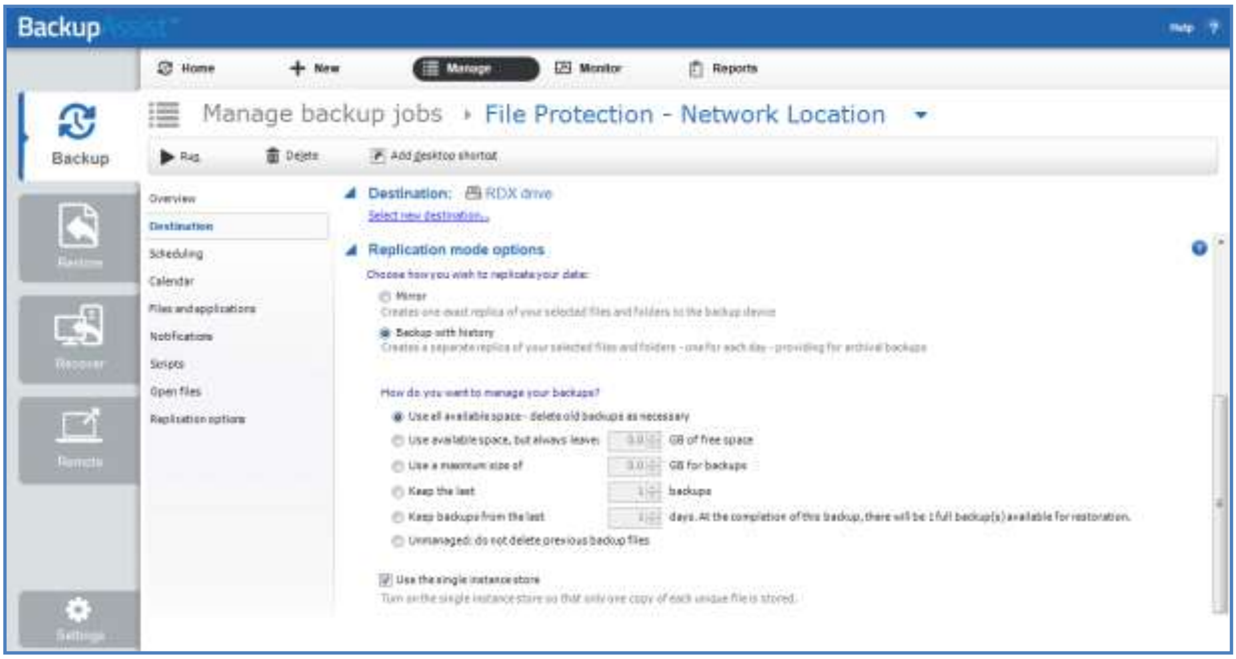
1. Select the backup job, and select *Run*.
2. You will be prompted to *Rerun a past backup* or to *Run a future backup now*.
3. When the backup job starts, the screen will change to the *Monitor* view.
4. Once the backup has been completed, select the *Report* button and review the results.

## 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**.



Manage backup jobs › File Protection - Network Location

Destination: RDX drive

Select new destination...

Replication mode options

Choose how you wish to replicate your data:

○ Mirror

Creates one exact replica of your selected files and folders to the backup device

● Backup with history

Creates a separate replica of your selected files and folders - one for each day - providing for archival backups

How do you want to manage your backups?

● Use all available space - delete old backups as necessary

○ Use available space, but always leave: 0.0 GB of free space

○ Use a maximum size of 0.0 GB for backups

○ Keep the last 1 backups

○ Keep backups from the last 1 days. At the completion of this backup, there will be 1 full backup(s) available for restoration.

○ Unmanaged: do not delete previous backup files

☑ Use the single instance store

Turn on the single instance store so that only one copy of each unique file is stored.

**Figure 10: 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 user guide

## 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 Add-on* and the *Hyper-V Advanced Add-on* licenses.

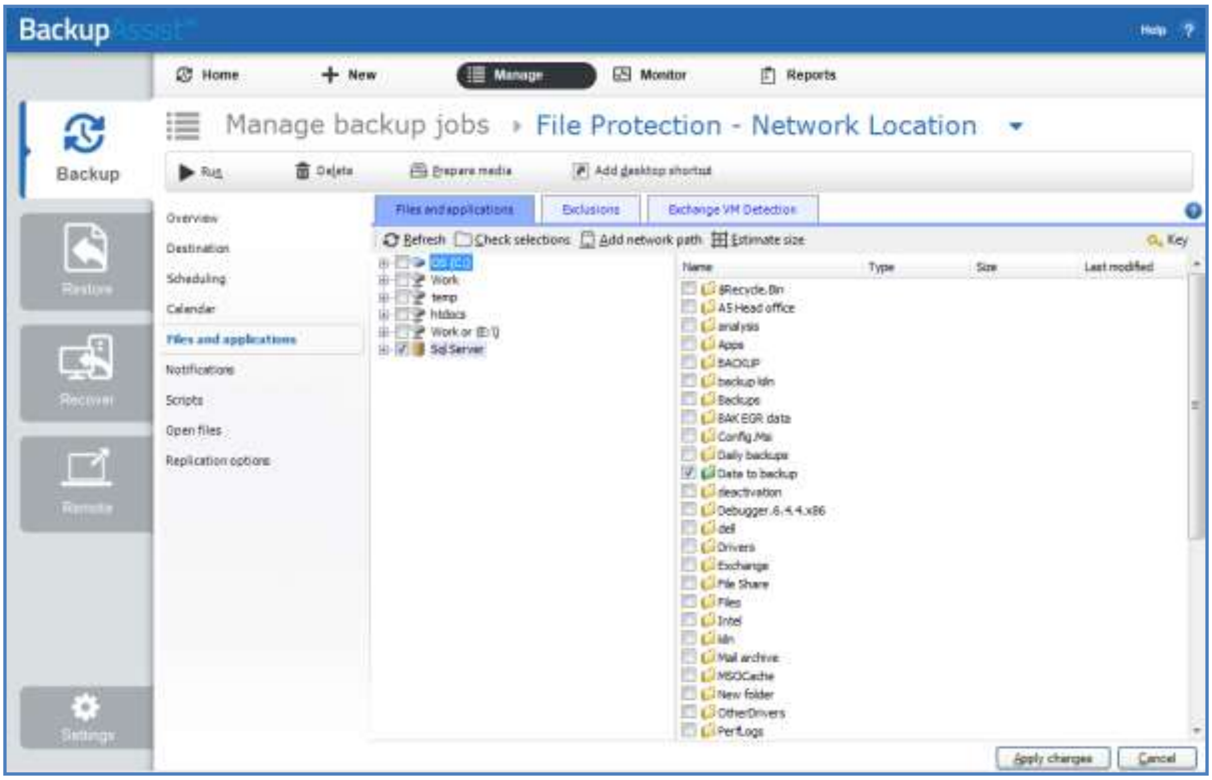


**Figure 11: Manage backup jobs screen – File and applications option**

# 7. File Protection backup report

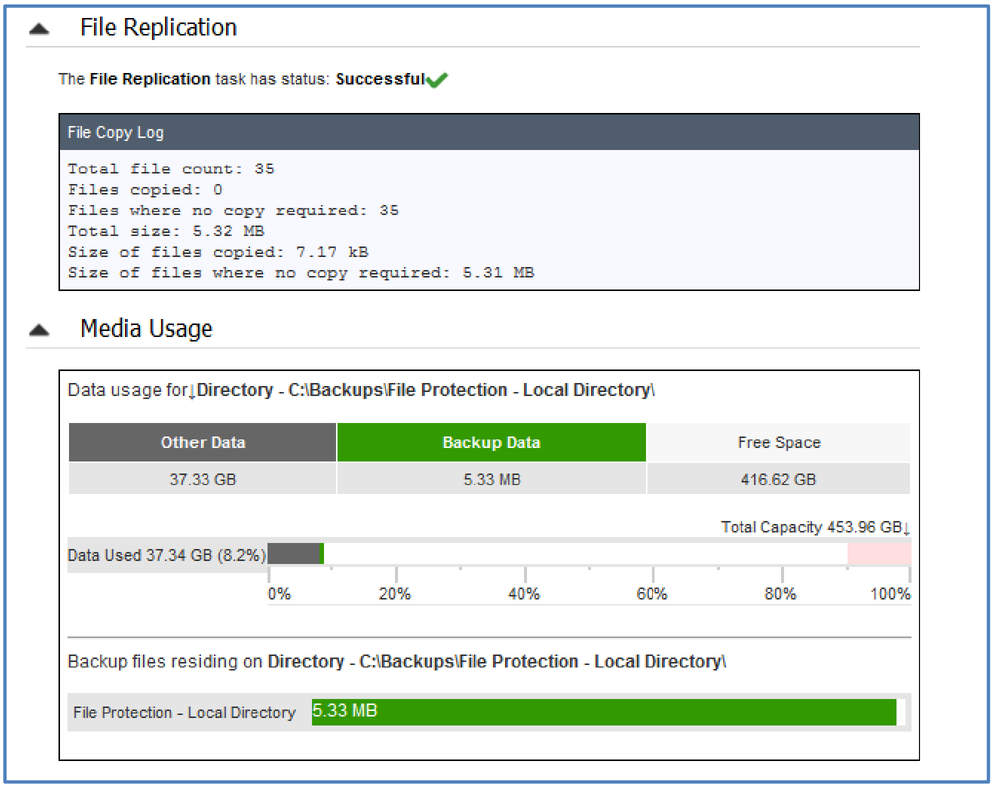
BackupAssist File Protection reports are very similar to those created from other backup engines. Some sections, however, are unique to File Protection and explained in greater detail below.

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.



File Replication

The **File Replication** task has status: **Successful** ✓

File Copy Log

```
Total file count: 35
Files copied: 0
Files where no copy required: 35
Total size: 5.32 MB
Size of files copied: 7.17 kB
Size of files where no copy required: 5.31 MB
```

Media Usage

Data usage for **Directory - C:\Backups\File Protection - Local Directory**

| Other Data | Backup Data | Free Space |
|---|---|---|
| 37.33 GB | 5.33 MB | 416.62 GB |

Total Capacity 453.96 GB

Data Used 37.34 GB (8.2%)

Backup files residing on **Directory - C:\Backups\File Protection - Local Directory**

File Protection - Local Directory 5.33 MB

**Figure 12: File Protection backup report**