

BackupAssist™ v8

System 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	2
Documentation	2
Licensing	2
Operating system considerations.....	2
2. Backup considerations.....	3
Exchange VM Detection	3
Incremental image backups.....	3
Restore vs. Recovery	3
3. Creating a System Protection backup	4
4. Restoring from a System Protection backup.....	7
5. System Protection backup management	10
Destination.....	10
Files and applications	11
Scheduling	11
Imaging options	12
6. System Protection backup report	13

1. Overview

Windows Server Backup uses drive imaging technology for data protection. BackupAssist allows you to take advantage of this backup functionality. The result is a feature-rich, reliable and cost-effective data and disaster protection solution.

Documentation

More information on System Protection can be found in the [System Protection whitepaper](#).

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

Other BackupAssist documentation includes:

- To perform a system recovery using an image backup, see the [Recover Tab Whitepaper](#)
- To protect Hyper-V environments, see the [System Protection for Hyper-V 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](#).

Licensing

System Protection is a standard feature included with the BackupAssist license, and requires a BackupAssist 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](#).

Operating system considerations

BackupAssist System Protection creates an image backup for:

- Windows 7
- Windows 8 and 8.1
- Windows Server 2008R1/R2
- Windows Server 2012/R2.

For a full list of the platforms supported by BackupAssist, see our [System Protection tour](#) page.

Note: System Protection cannot incrementally back up data from a ReFS formatted drive (source). This means a full backup of all selections will take place each time the backup job runs.

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.

Incremental image backups

System Protection creates a full backup the first time it runs. Subsequent backups are incremental. To create an incremental backup, BackupAssist scans and compares the data to be backed up and the data in the destination image to see what data changed. The process can take a long time, but when **Enable image tracking** is selected, System Protection backups record the changes to the data using a virtual snapshot. This means the backup job only needs to look at the snapshot to see what data changed. The result is significantly faster backups. *Enable image tracking* is enabled by default under the *Settings* tab > *Windows Setting* screen > *Incremental backup tracking for System Protection* section.

To learn more, visit our article on making [faster incremental image backups](#).

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.

System Protection can create the image backup used in the recovery process. It can also create an image backup to protect data and applications so they can be restored onto a functioning computer (as explained in this whitepaper). These two capabilities make System Protection a powerful and versatile backup solution. It is important to understand the difference between restore and recover so that both solutions can be implemented effectively.

The [Recovery using a System Protection backup](#) section of this whitepaper, explains how a System Protection image backup is used in the recovery process.

For more information on data recovery, see the [Recover tab & RecoverAssist Whitepaper](#).

3. Creating a System Protection backup



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

Launch BackupAssist and follow the steps outlined below:

1. Select the **Backup** tab, and click **Create a new backup Job**
2. Select **System 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 [BackupAssist settings](#), whitepaper 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.

A System Protection backup creates an image backup that can be used to restore data, or recover your entire system when used with a bootable, recovery media. For this reason there are two selections to choose from:

- **Back up the Entire System.** This option will create an image of your system that can be used to perform a full *recovery* of your computer. The Critical Volumes are selected by default and include *bare-metal* recovery data.
- **Back up selected items only.** This option is used if you only want to create a backup of files, folders and applications. The option will allow you to deselect *Critical Volume's* (bare-metal) and select specific VSS containers and drives.

You can select specific data within a drive (e.g. C:) if the back up is to a *Removable* disk. To do this, modify the backup job after you save it using the *Manage* menu on the *Backup* tab.

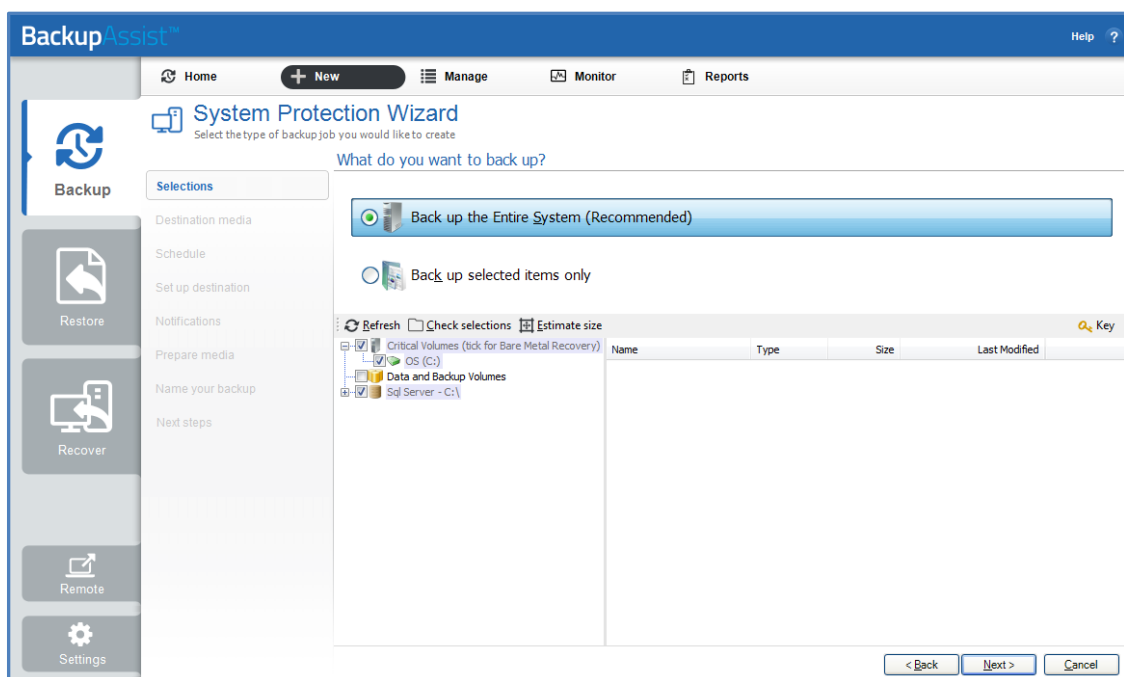


Figure 1: System Protection backup – data selection screen

The data selection screen includes the following options:

- **Critical Volumes:** This data is required for a bare-metal backup. The backup can be used with a bootable recovery media to recover your computer, after hardware has been replaced or an operating system failure has occurred and your computer can no longer start itself.
 - **Estimate size:** This tool is useful for planning the backup destination space.
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.

The **Enable Data container**, option is available for the following destinations: *RDX drive*, *Local hard drive*, *Network location* and *External disk*. A Data container is a file that the backups will be stored inside of. To learn more, see the [Data container resource page](#).

Note: System Protection backups on RDX drives cannot be used to restore individual files unless Data containers are used. This applies to Windows Server 2008R2 and later.

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

5. **Schedule:** This screen is used to select when and how often you would like a 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**.

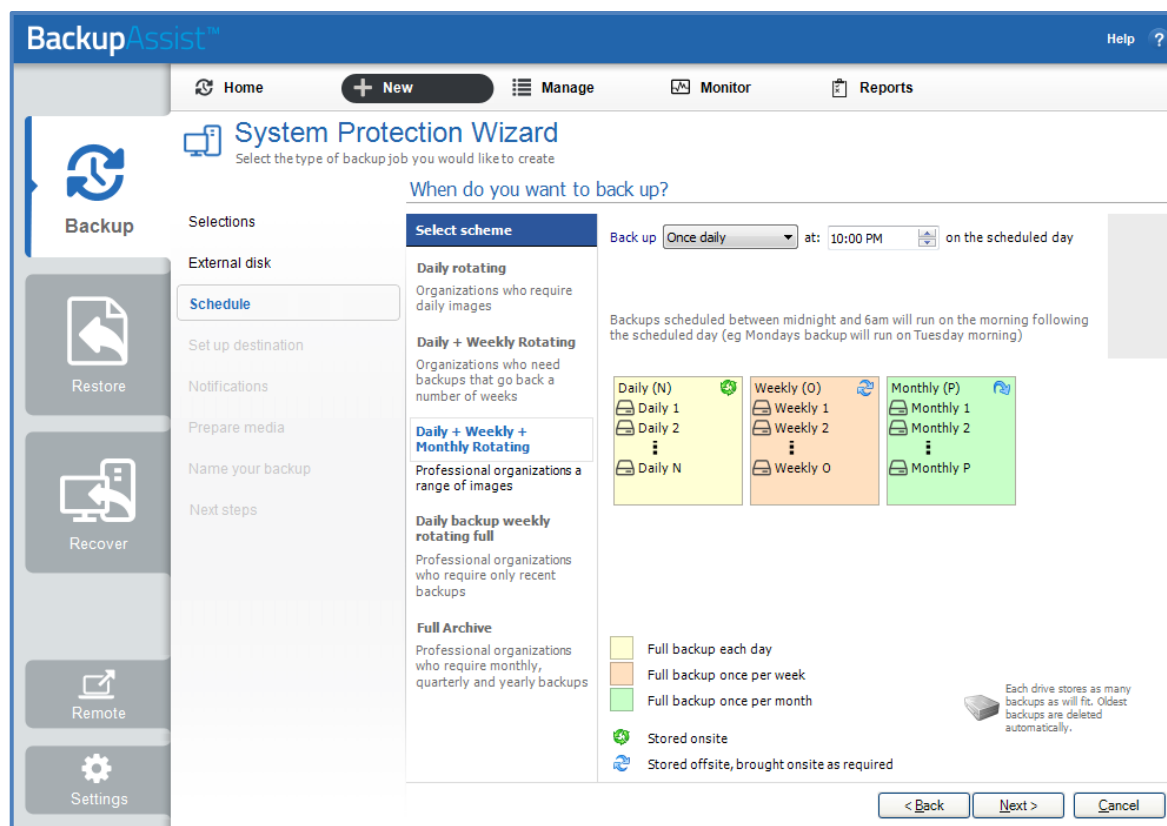


Figure 2: System Protection backup schedule - scheme selection

To learn more about System 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.
 - If your media is removable, you can set the media to eject after the backup job has finished.
 - Data containers are supported on Window Server 2008 R1/R2 and SBS 2008/2011 and later operating systems. If your destination is a Data container, the container size and location is set using this screen. It is important to review these settings to ensure they are correct, because the size of a Data container cannot be changed once the backup job has run. The *Use all available space* selection will use up to 2TB of space.

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

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:

- Select, **Add an email report notification**.
- Enter recipients into the **Send reports to this email address** field.
- 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.

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

- Select, **Let BackupAssist keep track of your media**.
- Select what you would like BackupAssist to do, *if the wrong media is inserted*.
- Select what you would like BackupAssist to do, *if new or unrecognized media is inserted*.
- Enter the name and drive designation to be used for each media device listed.
- Select **Prepare** for each media device listed.

BackupAssist will 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.

9. **Name your backup:** Provide a name for your backup job, and click **Finish**.
10. **Next Steps:** If you are creating a backup of your entire system for use in a recovery, you can use this option to launch the RecoverAssist builder and create and bootable recovery media.

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

Important: Once the *backup* has been created, the *backup verification* process will run. To learn about this process, visit our online [Backup verification page](#). **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 System Protection backup



This section provides instructions on how to *restore* data and applications from a System Protection image backup. The next section on page 17 explains how to an image backup is used in a system *recovery*.

To restore data from a **System 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.

Select the required Restore tool.

For a *System Protection* backup, the restore tool that will be displayed for both data and VSS applications is the **Restore Console**. How to use the *Restore Console* is explained in the next step.

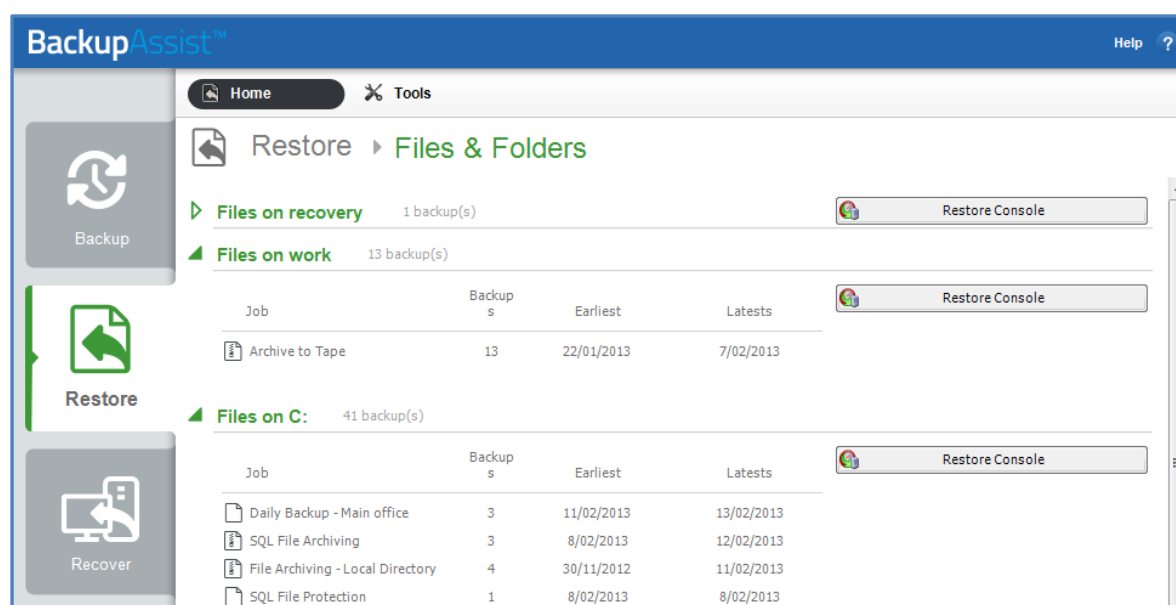


Figure 3: BackupAssist Restore Home page - selection results

4. Restore Console – backup and data selection

If selected, the *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.

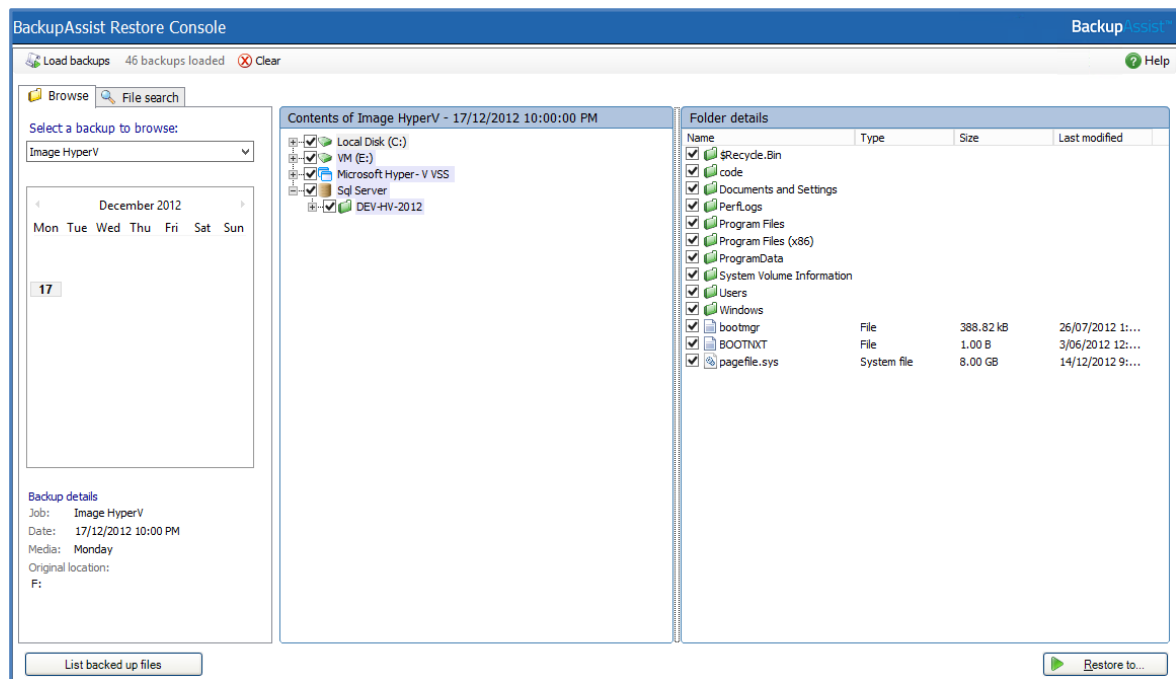


Figure 4: BackupAssist Restore Console – backup and data selection

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*.

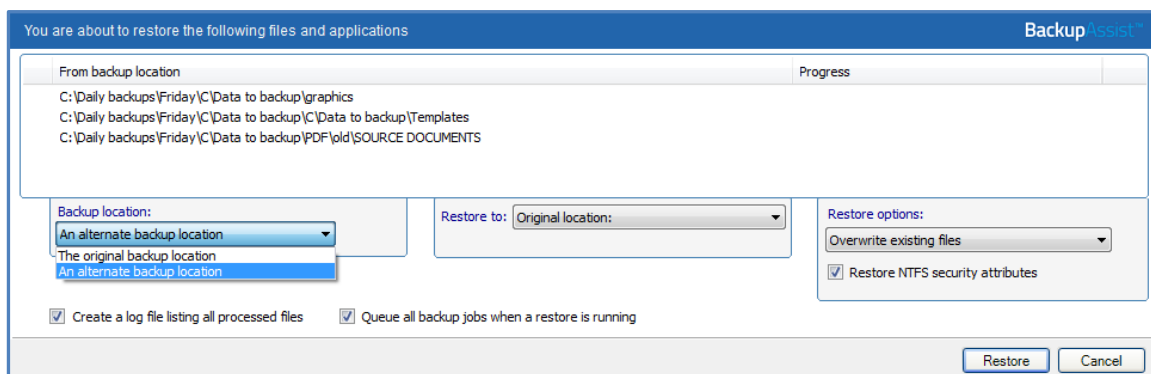


Figure 5: BackupAssist Restore Console – restore destination

- 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 one of the following: *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. A **Report** link will appear once the restore has finished.

- g. Select **Done**.

► **Your System Protection restore has now been completed.**

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

Helpful hint: If you backed up a Hyper-V machine using System Protection, and selected *Hyper-V* on the Restore tab's *Home page*, the **Hyper-V Granular Restore tool** will be displayed (as well as the Restore Console) and can be used to restore files from within a Hyper-V guest. For instructions on how to use this tool, see the [System Protection for Hyper-V whitepaper](#).

Helpful hint: BackupAssist automatically mounts Data containers when backups and restores are performed. However, there may be times when you want to do this manually. For example, if you want to check what is inside a Data container or have it available for another task. To manually mount a Data container, please refer to the steps outlined in our [blog article](#).

5. System 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.

Destination

Backup storage options

This option is used to determine how space is allocated for shadow storage on a removable backup destination. Shadow storage is used by VSS to store historical backup data from previous backup jobs.

There are two options available:

- **Use all available space for backup history**

With this option, BackupAssist makes all free space on the backup destination available for storing historical backups. The exact amount of the space used changes with time, depending on the amount of space used by the latest backup and other data.

- **Manually manage space for backup history**

With this option, Windows is used to determine the shadow storage size. You can allow Windows to automatically determine the size, or manually manage the size yourself using either the Windows Server settings or the vssadmin tool.

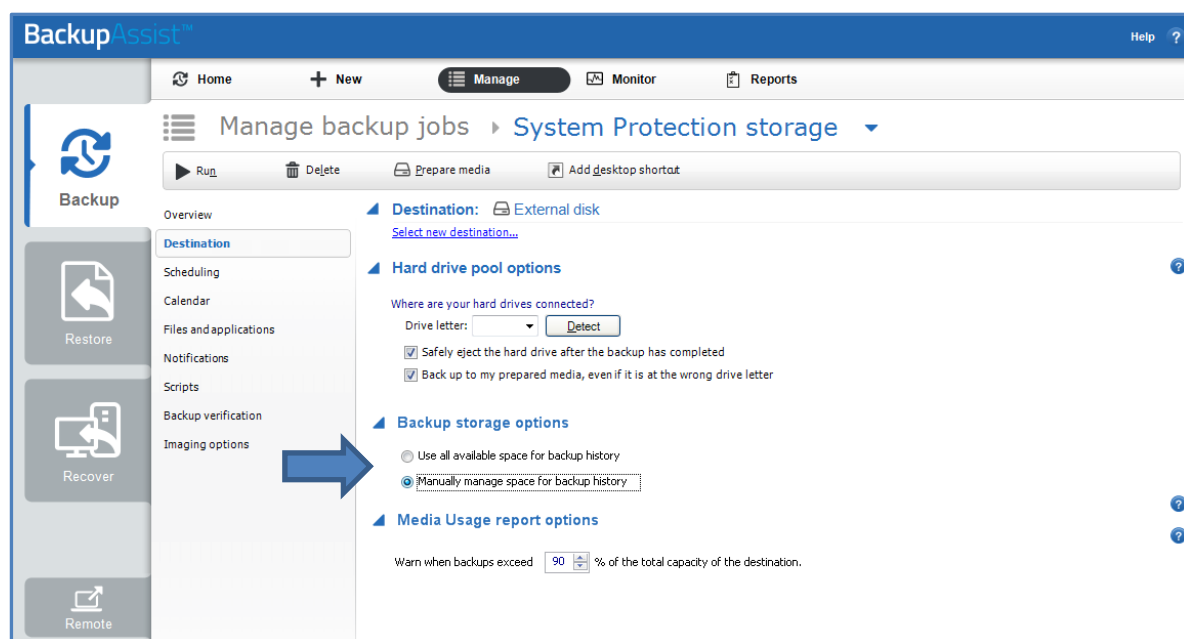


Figure 6: Imaging options - **NEW** Backup storage options

To set the size using the Windows Server settings:

- For Windows Server 2008, right click the drive and select Configure Shadow Copies
- For Windows Server 2012, open the drive's properties, select the *Shadow Copies* tab and access the *Settings*.

To set the size using the vssadmin tool:

- You can view the amount of space reserved for the shadow copy storage by running the command **vssadmin list shadowstorage** at an elevated command prompt.
- You can change the amount of disk space allocated to the shadow copy storage in GB or as a percentage of the disk, using the following commands:

```
vssadmin Resize ShadowStorage /For=X: /On=X: /Maxsize=XX%
vssadmin Resize ShadowStorage /For=X: /On=X: /Maxsize=XXGB
```

This will resize the limit to **XX** size for drive **X**:

The use all available space for backup history option is equivalent to "vssadmin Resize ShadowStorage /For=X: /On=X: /Maxsize=UNBOUNDED".

To see more VSS admin commands, please refer to this [Microsoft VSS admin resource](#).

For guidance on what the size should be, see our article on [Image backup destinations](#).

Data container options

You can modify the size settings of a Data container, if the container does not exist. For example, if the backup job has not been run or if the container has been manually deleted.

To modify the size select **Destination** and go down to **Data container options**:

- *Container size (GB)*: Use the up and down arrows to set the size of the Data container.
- *Use all available space*: Tick this box and all available space on the destination device will be used by the Data container, up to 2TB.

Files and applications

A new *System Protection* backup job will back up an entire disk or application. However, under the *Files and applications* menu item, you can modify your backup job by selecting specific files and folders, or individual components within a VSS application. The Volume Shadow Copy Service (VSS) is a Microsoft Service that creates a copy of an application's data (e.g. Exchange and SQL) so the data can be backed up without interfering with the application. BackupAssist will automatically detect *locally* running VSS applications and list them for selection during the **Destination** step of the backup job creation.

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. 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.

Scheduling

Selecting **Scheduling** will display the **Scheduling options**. You can use this screen to change the following settings for your scheme's daily backups: the time the backups run, how many times a day the backups run and the days of the week each backup runs on. If you selected a scheme with archive

backups (e.g. weekly, monthly), you can also 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*.

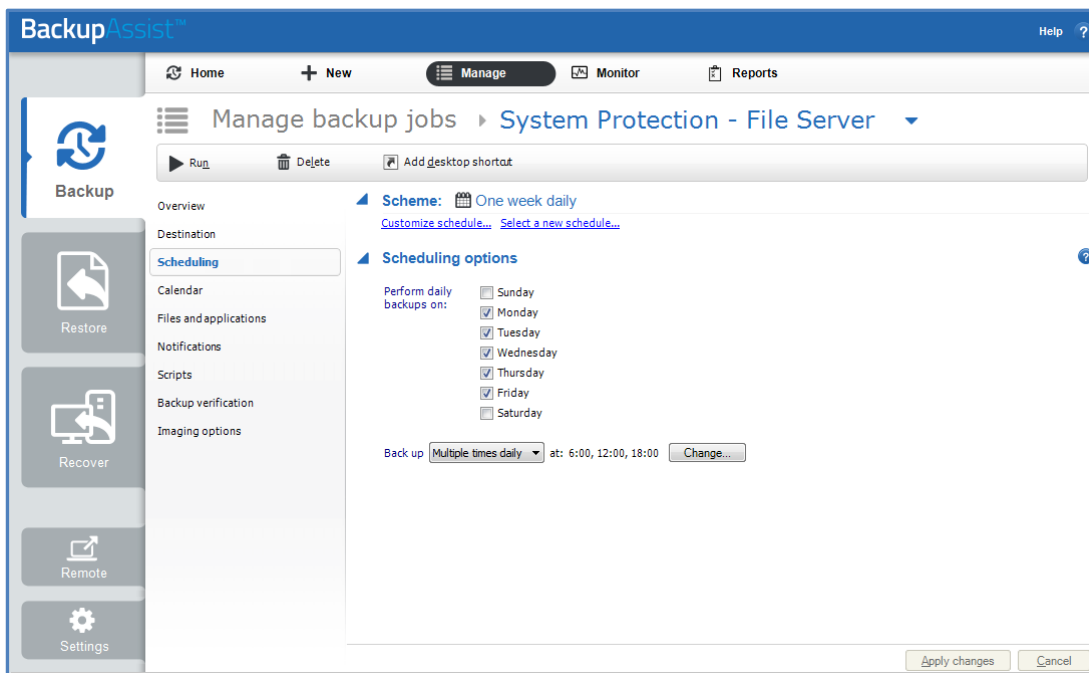


Figure 7: Manage Scheduling

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 scheduled backup within your current scheme. The customizations available will depend on the type of backup media used.

The *Method* selection can only be *Automatic*. This is because when a System Protection backup job runs, it scans the data, identifies what has changed and updates the backup image (VHD file) with the data changes. This means you have a full image backup that is updated incrementally. In some circumstances (a new destination or a change to the backup job) a full backup will still be performed.

Selecting the *Incremental Windows Image Backups* option on the *Settings* tab (under *Windows settings*) makes Windows flag any data that changes, so that when the System Protection job is run, it does not need to scan the data selection to know what has changed. This makes the backup a lot quicker, but there is a performance overhead between backups due to Windows keeping track of the changed data. In some circumstances (a change the job's settings or destination) a full scan may be required.

Imaging options

Imaging options provides configurations that can be applied to an existing System Protection backup.

Quick Catalogue - Selecting this option means the cataloging phase is done without mounting the VHD file. That means the catalogue does not contain details of the files and folders that were backed up, it only contains the other metadata associated with the backup, such as backup destination, VSS metadata and VSS snapshot ID. Because the quick catalogue does not contain an index of files and folders, you cannot search for a specific file or folder in the restore console. The restore console does allow you to browse the files and folders in the backup, however it does this by mounting the backup VHD rather than using the data in the catalogue. This means that the backup must be available.

6. System Protection backup report

The reporting capabilities of BackupAssist greatly enhance the reliability and accuracy of backup jobs.

Below are some key sections of the backup report:

Errors / Warnings Summary

Shows the status of the backup, plus a list of any warnings or errors. This is displayed at the top of the report so you can see any important messages quickly.

Destination Check

Shows any problems encountered with the backup's destination, such as incorrect backup media being detected (due to human error in the media rotation process) or if no media is detected at all.

Recovery Options

This section explains the BIOS, EFI and Hyper-V guest recovery options available for each System Protection backup.

Backups (Restore points)

This new section will list all of the backups you have on the backup destination. This will make it easy to see what restore options are available, and how far back you can restore from.

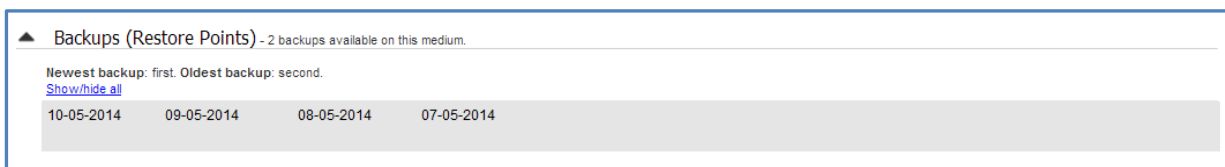


Figure 8: System Protection report - **NEW Backup (Restore points)**

Media usage

This section breaks down the space available at the backup destination for both the disk space and shadow storage. Shadow storage is used by VSS to store historical backup data from previous backup jobs. The example below shows the media usage report section for a Data container.

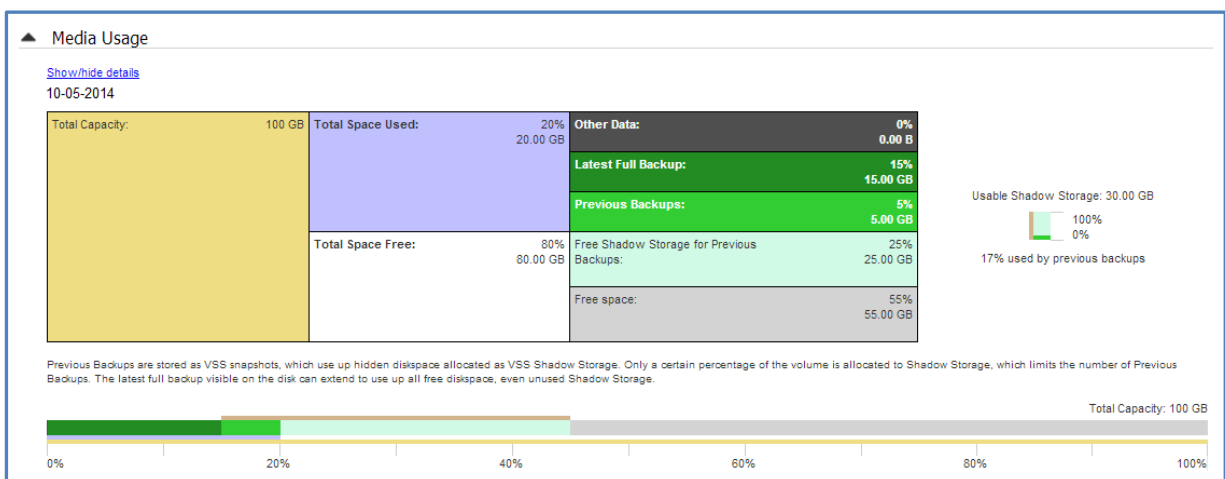


Figure 9: System Protection report – **NEW Media usage section**

Total Capacity of the backup destination is shown on the left. The usage graph breaks this amount down into **Used** and **Free** space, and then into more detailed allocations, such as shadow storage.