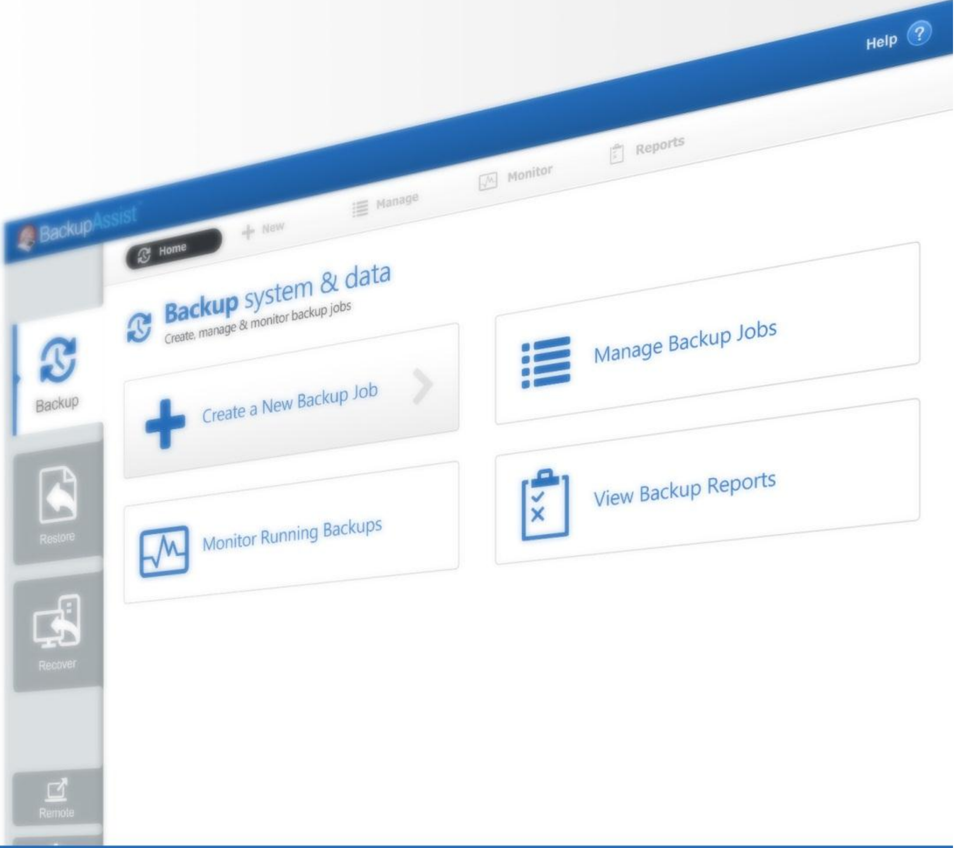


BackupAssist™

BackupAssist v7

System Protection

Whitepaper

backupassist.com

Cortex I.T.

Contents

1. **Introduction 2**
   - Licensing 2
   - Operating system considerations 2
   - Advantages and disadvantages of Windows Server Backup 3
   - BackupAssist: Enhancements to Windows Server Backup. 3
2. **Windows Server & BackupAssist comparison 4**
3. **System Protection backup strategy 5**
   - Last known recovery point 5
   - Multiple removable media 5
   - Running a test restore 5
   - Offsite storage of backup media 6
4. **Backup considerations 7**
   - Exchange VM Detection 7
   - VSS Application backups 7
   - Restore vs. Recovery 7
   - Windows SystemState 8
   - Data containers 9
5. **BackupAssist settings 10**
   - Backup user identity 10
   - Email server settings 10
   - Email address list 10
6. **Creating a System Protection backup 11**
7. **Restoring from a System Protection backup 15**
8. **Recovery using a System Protection backup 18**
   - Overview 18
   - RecoverAssist 18
9. **System Protection backup management 19**
   - Files and applications 19
   - Imaging options 19
   - Data container options 20
   - Scheduling 20
10. **System Protection backup report 21**
11. **Appendix I – Block level backup technology 22**
12. **Support and Resources 23**

1. Introduction

System Protection
For bare metal recovery

Method: Drive Imaging
Backup to Disk / iSCSI / NAS

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

This whitepaper explains how to protect your computer using BackupAssist System Protection, including how to create a backup, manage the configurations and restore both data and applications.

Documentation

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

- 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 Vista, 7, 8 and for Windows Server 2008R1/R2 and 2012/R2 computers. For Windows Server 2003, SBS 2003, Windows XP and older operating systems, the System Protection option will use NTBackup. NTBackup does not create an image backup, and it is therefore important to understand that the functionality available by having an image backup will not be available. For example, bare-metal recoveries and a Hyper-V granular restores require an image backup.

NTBackup can however be used to create a Windows SystemState backup and will use the System Protection features, including: backing up data, backing up VSS applications, reporting, scheduling and compatibility with different media types. The difference is the backups will be saved as a compressed data file, and not as an image. It is important to understand this when reading this document, and when planning your backup strategy.

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.

Advantages and disadvantages of Windows Server Backup

BackupAssist provides a fully-featured and flexible image backup solution. The Windows image backup solution has limitations as well as advantages, and both are outlined below.

Advantages	Disadvantages
• Fast disaster recovery from bare metal; you can create your own recovery CD. • Daily differential backups give you multiple points in time from which to restore. • Individual files can be restored. • Free with the Windows operating system**.** • Makes use of Volume Shadow Copy (VSS) and block-level backup technology.	• No file-based backups. • No support for tape drives. • Not suitable for long term data archiving or compliance purposes. • On Windows Server 2008/2012 you have to select entire drives to backup and cannot choose individual directories (unless the destination is a NAS or RDX drive.

Many of these disadvantages can be overcome using the backup solutions in BackupAssist.

BackupAssist: Enhancements to Windows Server Backup.

System Protection adds significant management features that improve on Windows Server backup. These improvements make it easier to configure custom backup jobs. These improvements include:

- **Scheduling**: There are limitations when using the built-in Microsoft scheduler. BackupAssist adds significant management features to make sure that the backups are run correctly and reliably.
- **Support for VSS applications**: BackupAssist provides fully integrated support for Volume Shadow Copy Service (VSS) applications such as Exchange Server, SQL Server, SharePoint and Hyper-V.
- **Support for removable disk cartridges**: BackupAssist can back up to and restore from devices such as Tandberg QuikStor, Quantum GoVault and RDX.
- **Support for fixed disks**: BackupAssist allows you to backup to local fixed disks, eSATA disks and NTFS NAS destinations, which is not supported in the built-in Server 2008 and SBS 2008 wizards.
- **Removable HDD management**: BackupAssist will safely eject your HDD after a backup has completed and automatically remap a drive letter if it is incorrectly assigned.
- **Media rotation schemes**: The BackupAssist scheduling function allows you to select from different rotation schemes and to customize those schemes.
- **Media reminders**: BackupAssist will send reminder messages to the backup operator on what drive to connect to the computer so that the media rotation strategy is correctly followed.
- **Reporting**: Reports are emailed to selected recipients each time a backup job runs. These reports contain important details and statistics on the backup result.
- **Scripting**: With BackupAssist you can write scripts to run before and after a backup, including conditional scripts that run specific commands based on whether the backup failed or succeeded.
- **Monitoring**: Monitor the “live” progress of your backups – with BackupAssist you can monitor the live progress using an Administration Console.
- **Remote management:** The BackupAssist Central Administration console allows you to monitor and administer all of your BackupAssist computers from one location in real-time.

2. Windows Server & BackupAssist comparison

The Microsoft Windows Server 2008 and Small Business Server (SBS) 2008 provide a fully functional backup solution, but lack many of the features required for a comprehensive backup strategy. BackupAssist enhances the Microsoft Backup solution with a fully-featured, saleable and flexible suite of technologies. The chart below provides a detailed listing of these features.

Product comparison

Feature	Server 2008	SBS 2008	BackupAssist
Functionality			
Easy setup and scheduling	✓	✓	✓
Multiple backup jobs	✗	✗	✓
Real time monitoring	✗	✗	✓
Event log backup results	✓	✓	✓
In-built media rotation schemes	✗	✗	✓
Hardware support			
Support for USB HDDs	✓	✓	✓
Support for eSata disks	✗	✗	✓
Support for removable disk (RDX)	✗	✗	✓
Detect & inject HDDs before backup	✗	✗	✓
Safely eject HDDs after backup	✗	✗	✓
Remote management			
Monitor remote backups from a console	✗	✗	✓
Run backups remotely	✗	✗	✓
Start a remote session using the backup client	✗	✗	✓
Reporting and notifications			
Remind operator to insert media	✗	✗	✓
Maintenance messages	✗	✗	✓
Reports emailed to administrator	✗	✓	✓
Notification if user inserts wrong disk	✗	✗	✓
Detailed backup log	✗	✗	✓
Media usage report	✗	✗	✓
Scripting			
Run script before / after backup	✗	✗	✓
Run script unconditionally after backup	✗	✗	✓
Run script if backup succeeded or failed	✗	✗	✓

3. System Protection backup strategy

A good backup strategy is important to protect your company in every recovery scenario. There are five critical points to consider when setting up a backup strategy. Each point is described below.

Last known recovery point

One very important factor to consider is that your backups should provide you with a **last known good point** for recovery. Consider the following story.

> A hacker has found and exploited a security vulnerability in the operating system, modified some system settings and uploaded a back-door for future access. The entire system is now compromised and the system has been infested with malware and Trojans. The actions taken by the hacker are unknown, and there is no easy way to know what changes were made.

Some malware / virus infections may go undetected for several days. If the infection happened 3 days ago, and the only backup available is last night's backup, then the backup is effectively useless. However, if there is a backup from 3 days ago (just before the infection) then the server can be restored to the *last known good point*.

It is not always possible to know when your *last known good point* is – so for this reason it is important to have a variety of backups from different points in time. That means you need more than one backup medium (i.e. more than one disk to store your backups). These disks are then commonly divided into different sets - one set of backup media (in this case, disk) for daily backups, and another set of backup media for weekly backups. BackupAssist also gives you the option of having monthly and yearly backup disks for additional security.

Multiple removable media

When using a backup destination such as USB hard drives or RDX drives, it is recommended that multiple disks/cartridges are used as part of the rotation strategy. Due to the nature of Windows Imaging backups, the number of different points in history that we can restore from is correlated to the number of devices used for the backups.

Backup Device	Recommended Number of Disks/Cartridges
USB Hard-drive	3 to 5 or more
RDX drive	5 or more

Running a test restore

In addition to running backups successfully, the integrity of backups should be checked, on average, once a month to ensure that they are restorable. By frequently running a test restore, you will be able to confirm that the backups can be used in a real restore scenario. Test restores also give you practice in the restoration process so that you are aware of the steps and what is required.

Offsite storage of backup media

In order to protect your company data from physical events like natural disasters or theft of hardware, backups should be taken offsite and kept in a secure location. Although it is important to keep some backups on-site to be able to restore data quickly, is equally important to keep at least one backup a week off-site.

Keeping backups off-site enables users to restore their servers in the event of any such disasters. The convenience of being able to restore data immediately from on-site storage of backups should not deter users from also storing backups off-site.

> A hurricane has gone through the city's business district and destroyed everything its path. Your company has been severely affected - all office equipment such as servers, personal computers, and lap-tops has been destroyed beyond salvage. The IT department implemented a backup strategy earlier in the year covering all the computers on the network. Unfortunately, all the backups were stored in a safe on-site and were also destroyed in the hurricane.

We suggest that you store the daily backups on-site and the weekly backups off-site. (BackupAssist can even help you manage off-site backups using the Internet. For more information, visit our online product page: http://www.backupassist.com/BackupAssist/tour_Rsync.html)

Imaging backup scenarios

Imaging daily

When running a Windows Imaging backup daily to a removable device, a good strategy would be to use 5 disks – for example, 2 for daily backups and 3 for weekly backups. The two *daily* disks can be rotated across the daily backups (i.e. Monday and Wednesday's backup goes to Daily 1 and Tuesday and Thursday's backup goes to Daily 2). The three *weekly* disks can be swapped across the three weeks and the most recent weekly backup can be stored off-site. With multiple disks for the backups, you have a variety of restore points from which to choose. It is possible to alter this strategy – for example, 3 daily backup disks and 2 weekly disks, or 3 daily disks, 1 weekly disk and 1 monthly disk.

Imaging weekly

If there are constraints (excessive amounts of data, limited physical access to the server or procedural constraints) that make it impossible to image your system daily, it is still possible to have an effective backup system in place by running a Windows Imaging backup on a weekly basis.

For example, this scenario will still enable you to recover a system in the event of a disaster:

- Perform the drive imaging backups on a weekly basis (with 3 or more drives to enable media swapping).
- Use a different backup technology, such as a BackupAssist File Protection, to back up your applications and data on a *daily* basis.

In the event of a disaster, you can restore your system to the last image and then "roll forward" your data and applications from your daily backup.

4. 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.

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.

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.

Data containers

The backup

BackupAssist *System Protection* creates image backups that can be used to restore and recover your data. These backups can be full or incremental, and the Windows Volume Shadow copy Service (VSS) maintains historical information so that each backup can be restored from.

Key points:

- If you have Windows VSS on the data source, data can be backed up incrementally.
- Incremental backups overwrite the data in the image backup that has changed.
- Windows can create shadow copies (snapshots) of the data that was changed.
- Data that was overwritten by previous backups can be restored using a VSS snapshot.

The problem

On RDX drives and network destinations (e.g. NAS), shadow copies are not supported so Windows cannot maintain a backup history (snapshots of data that changed). This means restores can only be done from the last backup. A work around has been to put each backup into a different folder but this requires a full back up each time the backup jobs runs, which requires additional disk space.

Key points:

- Windows VSS cannot maintain historical information (snapshots) on a NAS or RDX device.
- Data can only be restored from the last backup.

The solution

BackupAssist overcomes these Network/RDX destination limitations, by implementing *Data containers*. A Data container is a VHD file that *System Protection* backups can be stored inside of. The Data container is created on the destination media and each time the backup jobs runs, the Data container is mounted and treated as a local disk. Because the container is seen as a local disk, Windows can maintain shadow copies of data that changed (was overwritten), so that it can still be restored from.

When using a Data container for System Protection backups to NAS and RDX destinations:

- Data (in the backup) that has changed can still be restored, because snapshots are maintained.
- Folders are not needed to provide different restore points, saving valuable disk space and time.

Other advantages

RDX granular restore: When Windows detects an RDX drive, it will compress the data that is being backed up. This compression means that individual files cannot be restored. By using a Data container, Windows will see the destination as a local drive and not compress the data. BackupAssist will therefore be able to restore individual files from an image backup stored on an RDX drive.

Portable backups: Enable portable backups for RDX, network, external disk and local drive destinations.

On Windows Server 2008R2 and later, you can copy a backup image to another device, but only the last backup can be restored because you cannot copy the shadow copy (snapshot). If the backup is in a Data container, the snapshot can be moved and all backups can be restored from.

Supported systems

Data containers are supported on Window Server 2008 R1/R2 and SBS 2008/2011 and later operating systems.

To learn more, see the Data container resource page.

5. 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 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.

Windows Settings

System Protection creates a full image backup the first time it runs to a destination, but further backups will usually be incremental. This is achieved by scanning and comparing the data to be backed up and the data in the destination image to see what data changed, and only the data that has changed will be updated. Scanning can take some time, but can be avoided by enabling "incremental reading" using the option under the *Setting* tab > *Windows Settings* > *Enable Incremental Windows Image backups*.

6. 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 section above, BackupAssist settings, for guidance.

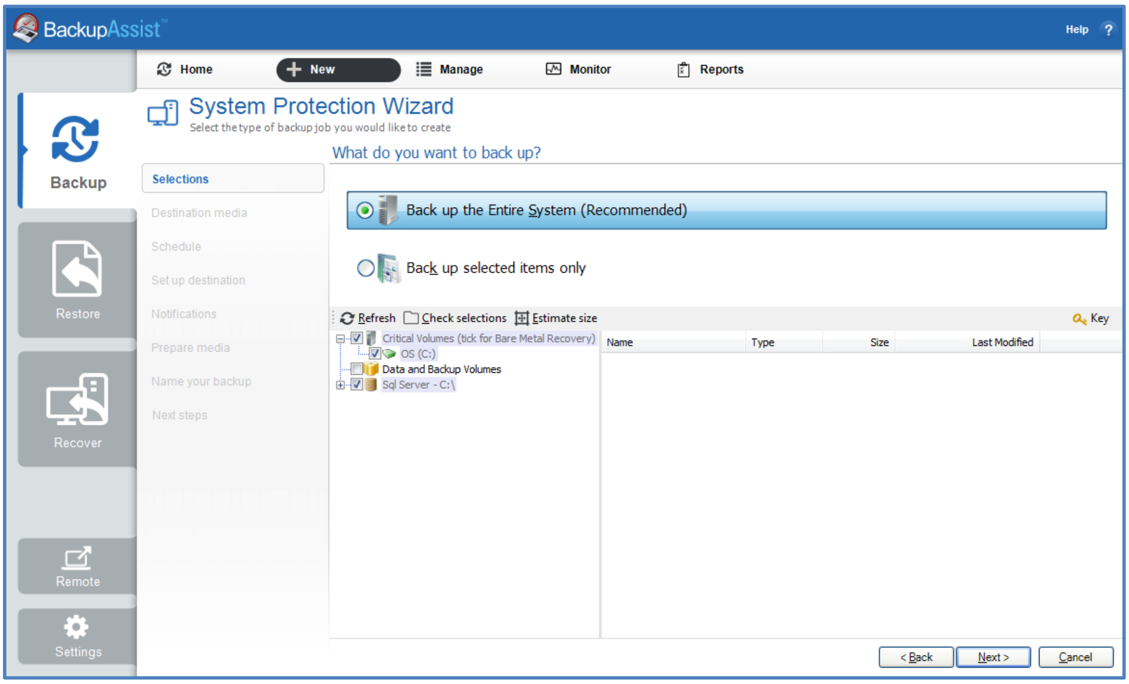
3. **Selections:** The selections screen is used to select the data and applications that you would like to back up. Any VSS applications detected will be displayed here as application directory apps.

   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 applications 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.



System Protection Wizard

Select the type of backup job you would like to create

What do you want to back up?

● Back up the Entire System (Recommended)

○ Back up selected items only

- ☑ Critical Volumes (tick for Bare Metal Recovery)
  - ☑ OS (C:)
- □ Data and Backup Volumes
- ☑ Sql Server - C:\

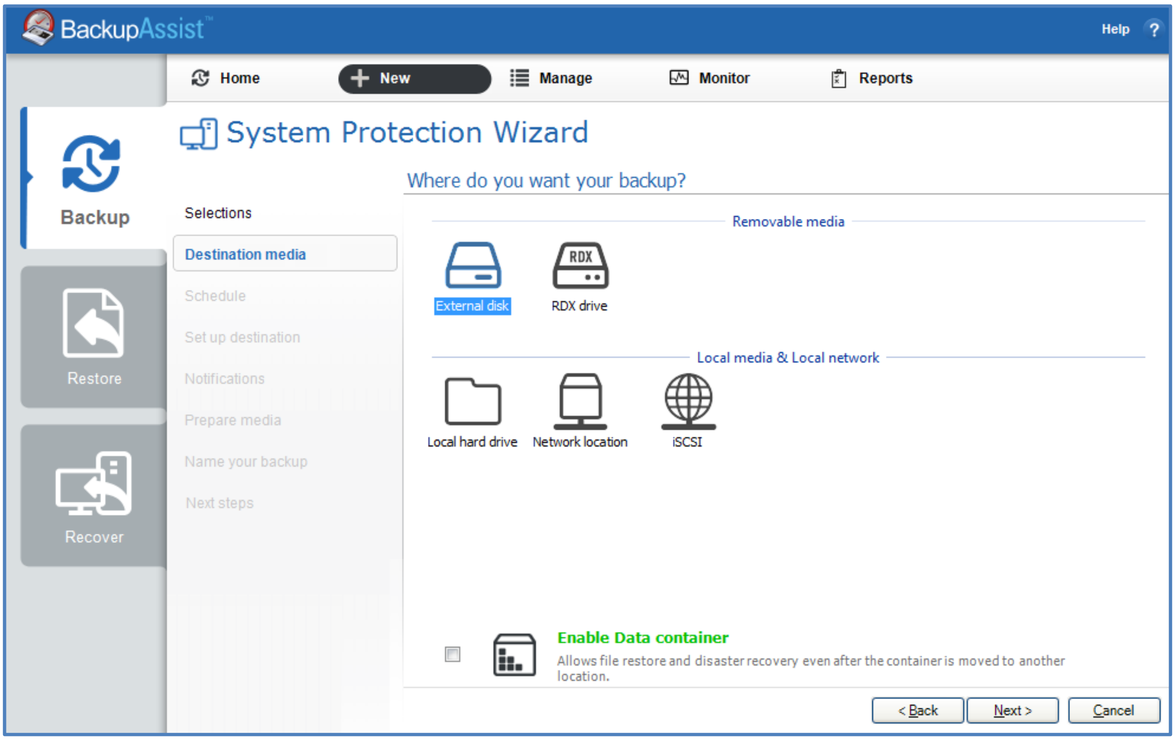
Figure 1: System Protection backup – data selection screen

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.

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



☐ **Enable Data container**
Allows file restore and disaster recovery even after the container is moved to another location.

Figure 2: System Protection – Destination media

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. The Data container is created on the destination media and each time the backup jobs runs, the container is mounted and treated as a local disk.

> **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.

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

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

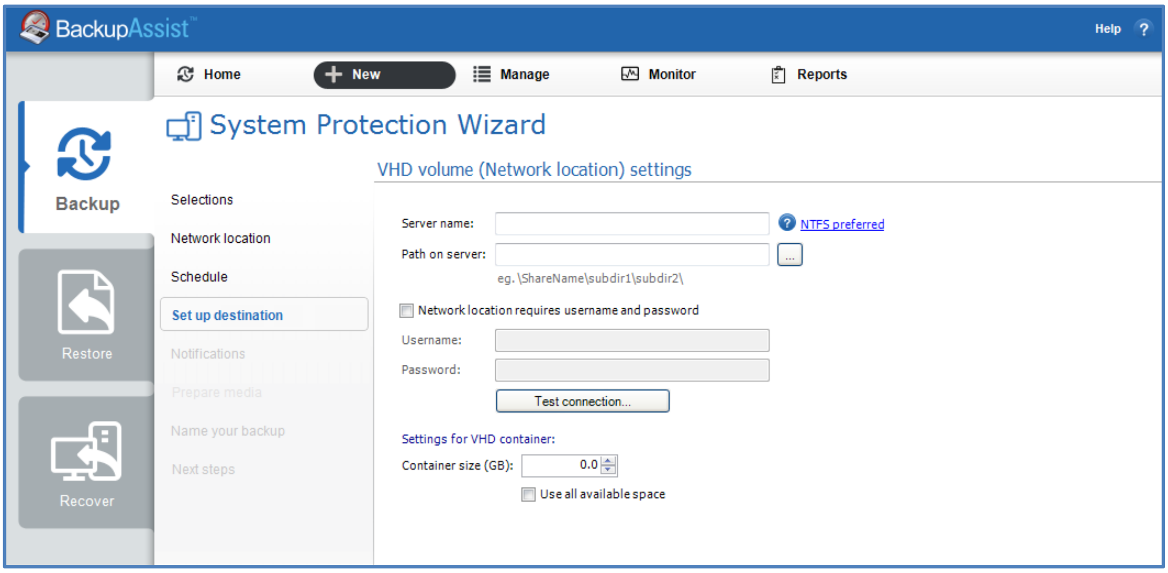
   For more information about schedules, refer to the Backup management: scheduling section.

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.

If your destination is a Data container, the container size and location is set using this screen.

- You will need to provide the destination path, the location where the container will be created.
- For an *RDX* or *External disk* destination, *Use all available space* will be selected by default. It is important to review this setting to ensure it is appropriate.
- For a *Local hard drive* and *Network location*, set the size manually by using the field provided, or select the *Use all available space* option.
- The size of a Data container cannot be changed once the backup job has run.
- The *Use all available space* selection will use all available space, up to 2TB.



System Protection Wizard

VHD volume (Network location) settings

Server name:

Path on server:

eg. \ShareName\subdir1\subdir2\

☐ Network location requires username and password

Username:

Password:

Settings for VHD container:

Container size (GB): 0.0

☐ Use all available space

Figure 3: BackupAssist System Protection – Set up destination screen

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

➢ **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 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:

   a. Select, **Let BackupAssist keep track of your media.**

   b. Select what you would like BackupAssist to do, *if the wrong media is inserted*.

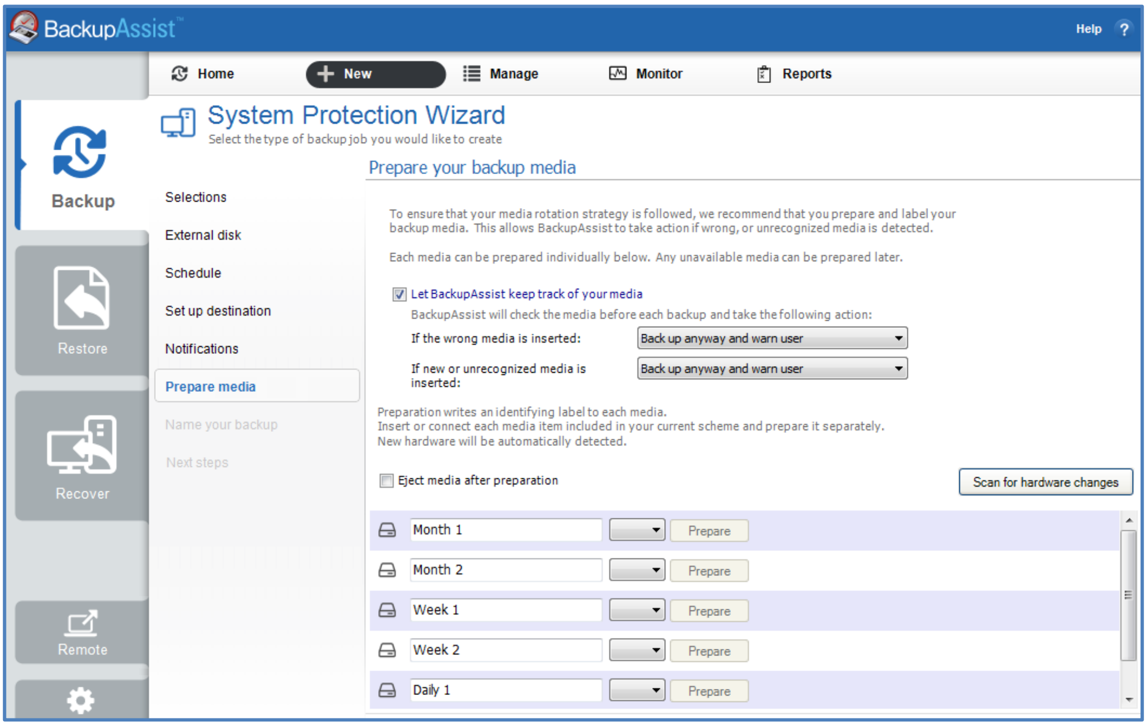
   c. Select what you would like BackupAssist to do, *if new or unrecognized media is inserted*.

   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.



System Protection Wizard

Select the type of backup job you would like to create

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: Back up anyway and warn user

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

☐ Eject media after preparation

Scan for hardware changes

Month 1 — Prepare
Month 2 — Prepare
Week 1 — Prepare
Week 2 — Prepare
Daily 1 — Prepare

Figure 4: System Protection – Prepare media selections

   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. See the section, System 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 System Protection backup.

7. 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.

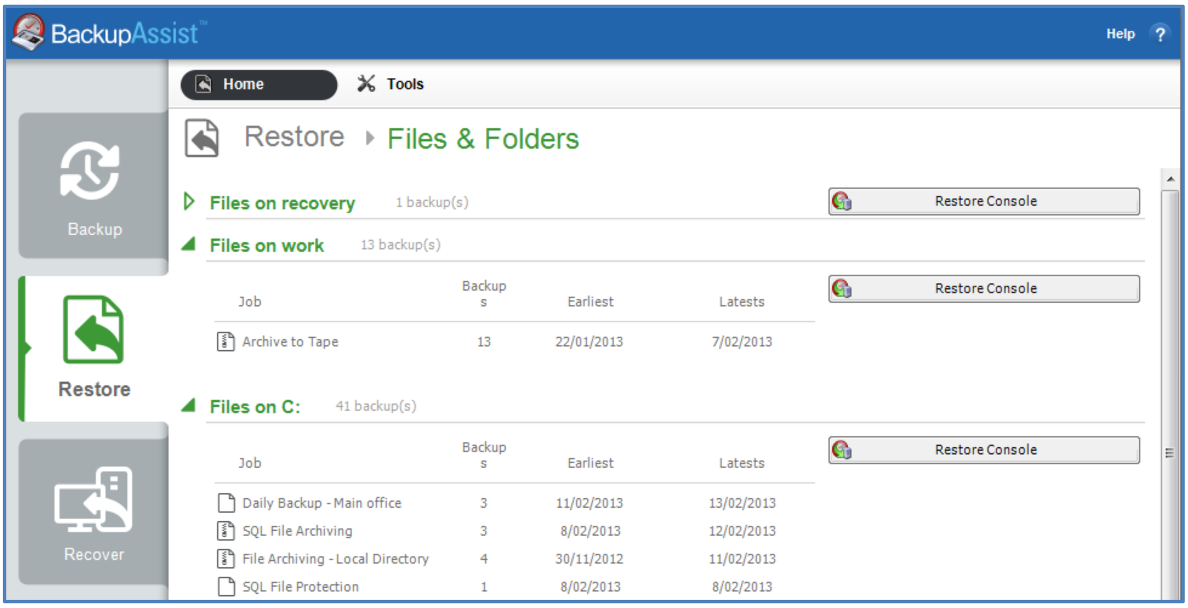
   - *Files and folders* will display all data backups and all VSS application backups.
   - *Applications* will display backups that contain VSS applications, and exclude data only backups.
   - *Exchange*, *SQL* or *Hyper-V*, will display all backups that contain the selected application. Selecting an 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.



Files on recovery 1 backup(s)

Files on work 13 backup(s)

Job	Backups	Earliest	Latests
Archive to Tape	13	22/01/2013	7/02/2013

Files on C: 41 backup(s)

Job	Backups	Earliest	Latests
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 5: 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.

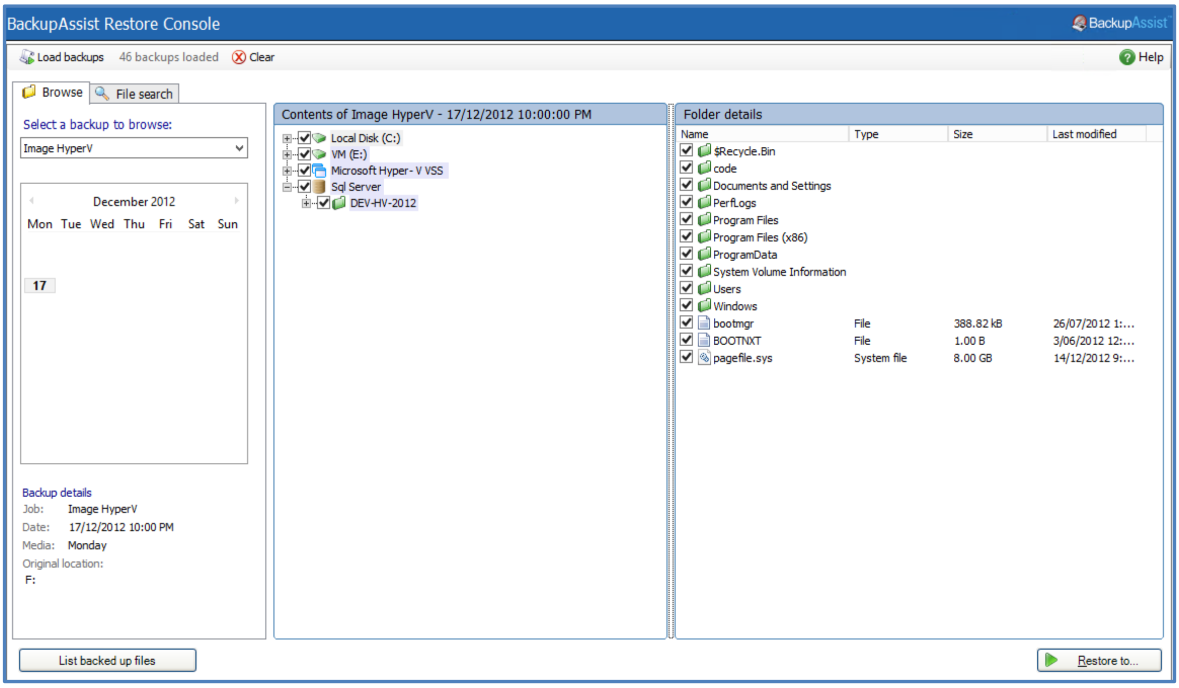
The Restore Console provides two tools to locate your data:

- 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.



Backup details
Job: Image HyperV
Date: 17/12/2012 10:00 PM
Media: Monday
Original location:
F:

Name	Type	Size	Last modified
☑ $Recycle.Bin			
☑ code			
☑ Documents and Settings			
☑ PerfLogs			
☑ Program Files			
☑ Program Files (x86)			
☑ ProgramData			
☑ System Volume Information			
☑ Users			
☑ Windows			
☑ bootmgr	File	388.82 kB	26/07/2012 1:...
☑ BOOTNXT	File	1.00 B	3/06/2012 12:...
☑ pagefile.sys	System file	8.00 GB	14/12/2012 9:...

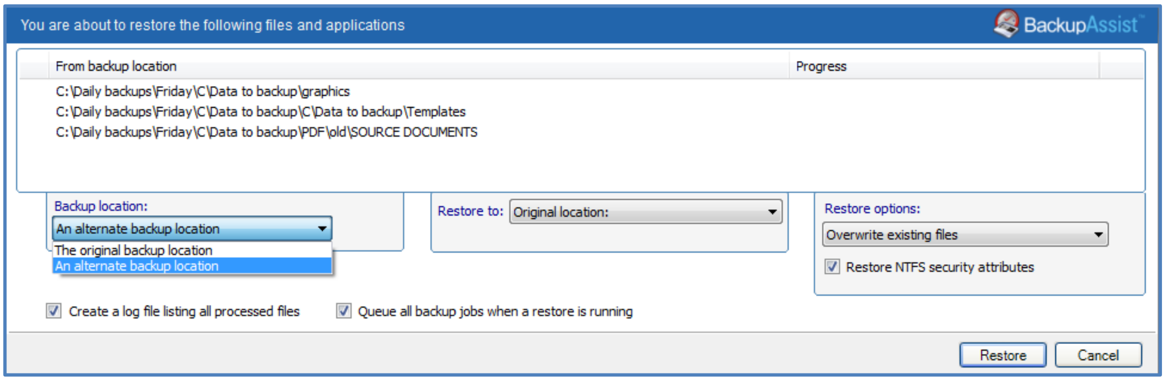
Figure 6: BackupAssist Restore Console – backup and data selection

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*.



You are about to restore the following files and applications

From backup location	Progress
C:\Daily backups\Friday\C\Data to backup\graphics	
C:\Daily backups\Friday\C\Data to backup\C\Data to backup\Templates	
C:\Daily backups\Friday\C\Data to backup\PDF\old\SOURCE DOCUMENTS	

Backup location: An alternate backup location
- The original backup location
- An alternate backup location

Restore to: Original location:

Restore options: Overwrite existing files

☑ Restore NTFS security attributes

☑ Create a log file listing all processed files

☑ Queue all backup jobs when a restore is running

Figure 7: 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 and 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.

8. Recovery using a System Protection backup

This section provides an overview of the BackupAssist recovery process. It is important to understand the link between a System Protection backup and RecoverAssist, because both technologies are used together to perform a recovery.

Overview

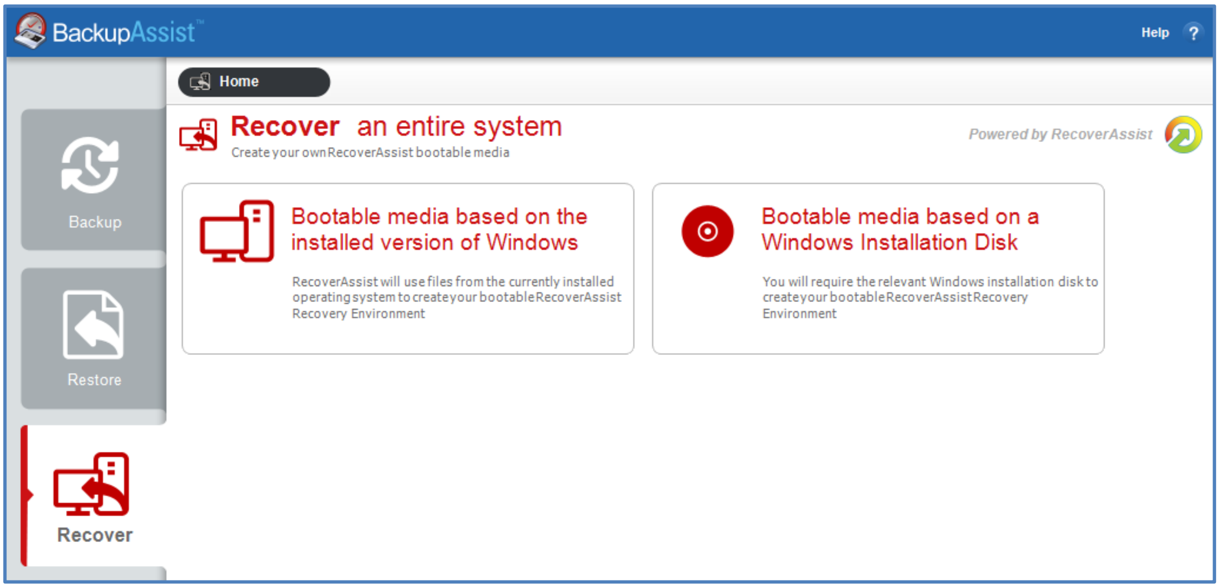
A recovery is the process by which a computer is recovered after hardware has been replaced or an operating system failure has occurred, and your computer can no longer start itself. To perform a recovery you need a bootable RecoverAssist media to start your computer, and an image backup containing the computer's operating system and data.

Once the computer has been started, RecoverAssist will create a recovery environment (on your monitor), which can access your System Protection image backup, and recover your operating system, data and any applications that were included in the image backup.

- ➢ System Protection creates an image backup of your entire system, known as a *bare-metal* backup.
- ➢ BackupAssist's RecoverAssist feature creates a customized, bootable recovery disk.

RecoverAssist

RecoverAssist is accessed through the BackupAssist Recover tab. It will use a wizard to create a customized, recovery disk using the local machine or a Windows installation disk.



Recover an entire system
Create your own RecoverAssist bootable media

Bootable media based on the installed version of Windows
RecoverAssist will use files from the currently installed operating system to create your bootable RecoverAssist Recovery Environment

Bootable media based on a Windows Installation Disk
You will require the relevant Windows installation disk to create your bootable RecoverAssist Recovery Environment

Figure 8: RecoverAssist media selection screen

For instructions on how to create a bootable *RecoverAssist* media, and how to use it with a *System Protection* backup, refer to the whitepaper, Recovery tab - RecoverAssist whitepaper.

The RecoverAssist whitepaper contains instruction on

- Bare-Metal backups and recoveries.
- How to create a bootable, Recovery media.
- How to recover a Windows Server using RecoverAssist and a System Protection image backup.

9. 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.

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.

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.

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.

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.

Scheduling

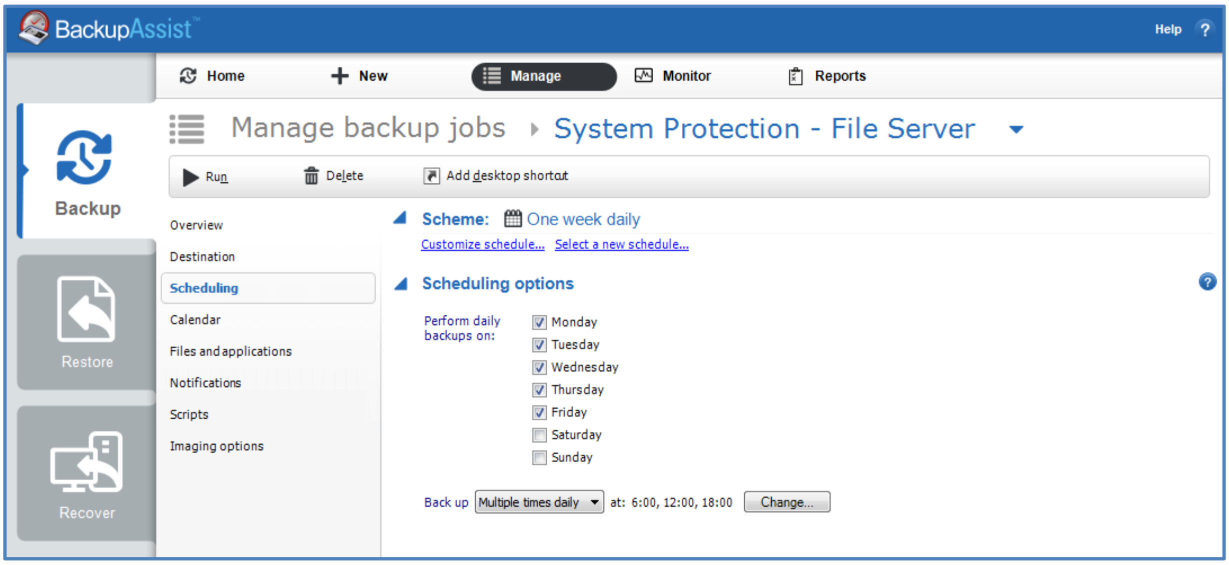
Selecting *Scheduling* will display the **Scheduling options.** You can use this screen to change the following settings for your scheme's daily backups: the time the backups run, how many times a day the backups run and the days of the week each backup runs on. If you selected a scheme with archive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

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.



Manage backup jobs ▸ System Protection - File Server

Scheme: One week daily

Scheduling options

Perform daily backups on:
☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☐ Saturday
☐ Sunday

Back up Multiple times daily at: 6:00, 12:00, 18:00 Change...

Figure 9: Manage Scheduling

10. System Protection backup report

The reporting capabilities of BackupAssist greatly enhance the reliability and accuracy of backup jobs. The reports show useful information such as how the backup process went and whether the media rotation scheme was followed.

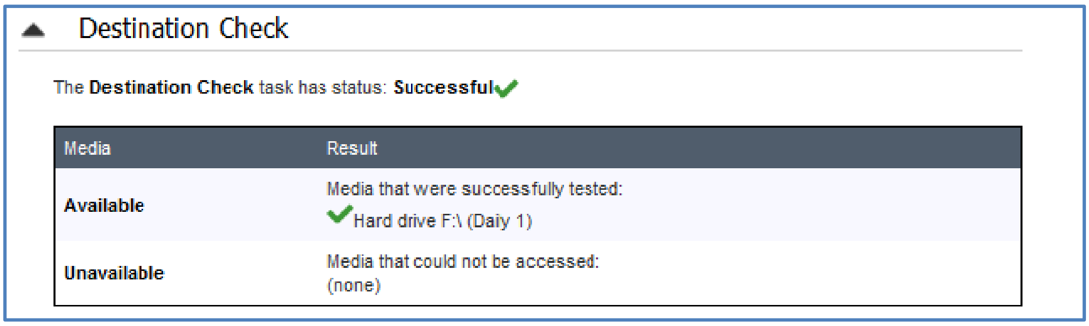
Below are some key sections of the backup report:

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.

Backup Job: Shows the backup job's vital statistics, such as the backup's duration and the media used.

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.

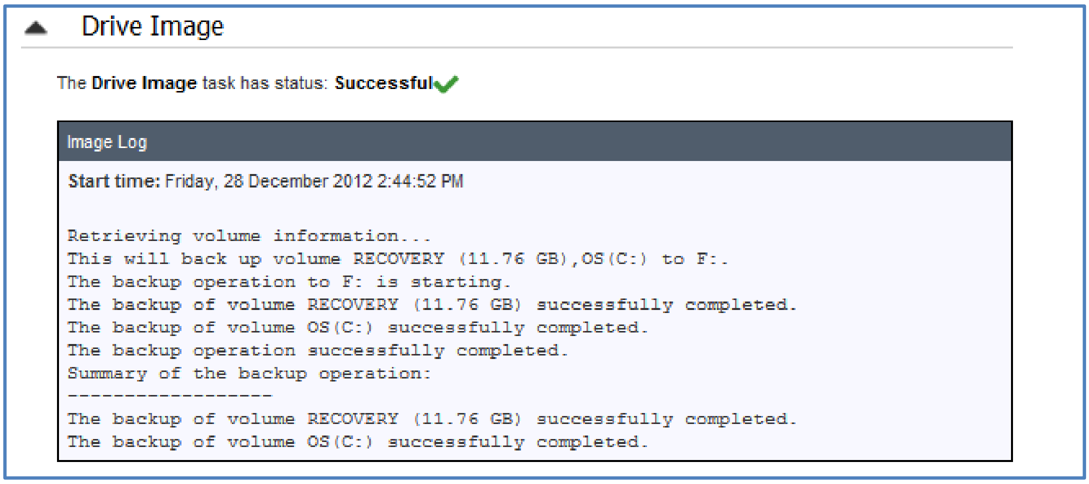


Destination Check

The **Destination Check** task has status: **Successful** ✓

Media	Result
Available	Media that were successfully tested: ✓Hard drive F:\ (Daiy 1)
Unavailable	Media that could not be accessed: (none)

Drive Image: Displays a log of what happened during the backup.



Drive Image

The **Drive Image** task has status: **Successful** ✓

Image Log

Start time: Friday, 28 December 2012 2:44:52 PM

```
Retrieving volume information...
This will back up volume RECOVERY (11.76 GB),OS(C:) to F:.
The backup operation to F: is starting.
The backup of volume RECOVERY (11.76 GB) successfully completed.
The backup of volume OS(C:) successfully completed.
The backup operation successfully completed.
Summary of the backup operation:
------------------
The backup of volume RECOVERY (11.76 GB) successfully completed.
The backup of volume OS(C:) successfully completed.
```

Media Usage

Shows media information, including:

- Space used by this backup
- Space used by previous backups (USB HDD / Local disk only)
- Free space on the media
- The actual size of a backup, with the compression ratio (RDX only)
- Backup versions on the media

11. Appendix I – Block level backup technology

The concept of full and differential backups through block-level backup technology is different to the traditional concept of full and differential backups found with file-based backups. When a backup of a disk is performed using block-level backup technology, the backup engine will create a full or a differential backup based on the comparison of the current state of the disk and any previous backups of that disk available on the backup destination. If there are no backups of the drive on the backup destination, the backup engine will create a full backup of the drive at that destination. Any subsequent backups of the drive to the same backup destination will be differential backups based on the differences between the current state of the disk and the backup on the destination.

Let us take a look at a situation where you are backing up C: drive to an external hard-drive on Monday (refer to *Monday's backup* in the figure below). If you imagine C: drive as being made up of blocks ***A***, ***B***, ***C***, ***D***, ***E***, ***F***, ***G***, ***H***, then the first block-level backup of C: drive to the USB hard-drive will be a **full backup**.

All subsequent backups of C: drive to the same external hard-drive will be differential backups where only the differences are backed up. If you run another backup of C: drive on Tuesday (refer to *Tuesday's backup* in the figure below), the differences will be backed up to the external hard-drive to create a new full backup.

Upon examination of the backup destination (refer to *Tuesday's backup* in the figure below), you notice that:

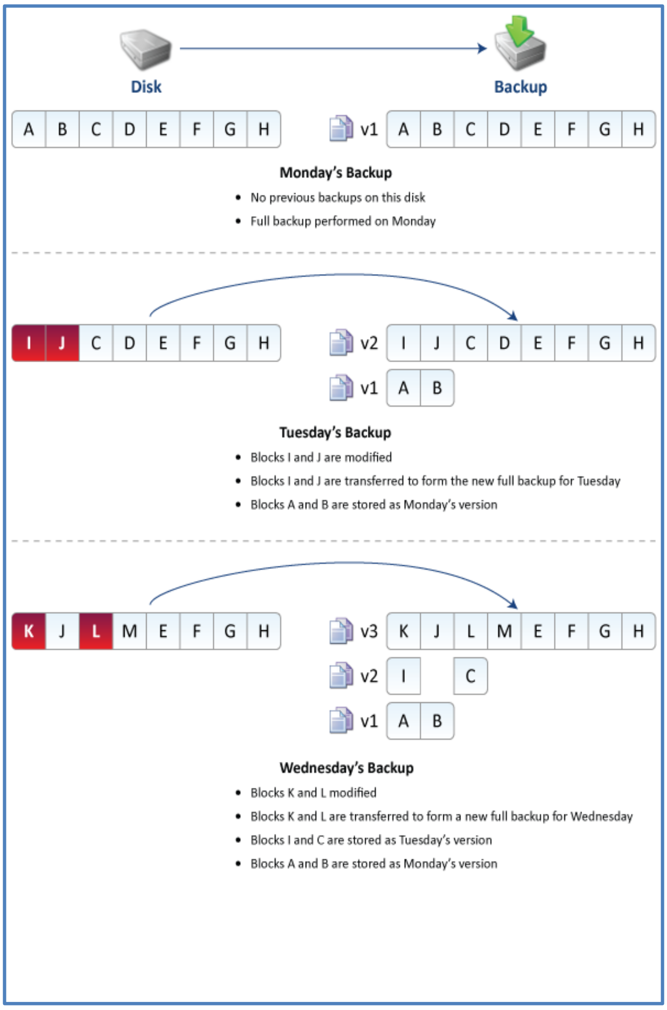
- The most recent full backup (***I***-***J***-***C***-***D***-***E***-***F***-***G***-***H)*** is always available.
- Past backup versions (***A***, ***B***) are always available.

Block-level backup is space efficient as only the block-level differences are stored. In addition, the previous backup versions get deleted as the drive gets filled up.

If you run a third backup of C: drive on Wednesday (refer to *Wednesday's backup*), the block-level backup engine will compare the current state of C: drive to the full backup on the destination and backup only the changes. Once again, the backup destination will show:

- Most recent full backup is always available. Now, it is ***K***-***J***-***L***-***M***-***E***-***F***-***G***-***H***.
- Past backup versions available.–(***A***, ***B***), (***I***, ***C***)

When the backup device is full, the oldest backups are automatically discarded. E.g. In the first backup v1 of blocks A & B would be deleted to free up space. If more space is required, the second backup of blocks I & C would be deleted next.



Monday's Backup

- No previous backups on this disk
- Full backup performed on Monday

Tuesday's Backup

- Blocks I and J are modified
- Blocks I and J are transferred to form the new full backup for Tuesday
- Blocks A and B are stored as Monday's version

Wednesday's Backup

- Blocks K and L modified
- Blocks K and L are transferred to form a new full backup for Wednesday
- Blocks I and C are stored as Tuesday's version
- Blocks A and B are stored as Monday's version

12. Support and Resources

Contacting Technical Support

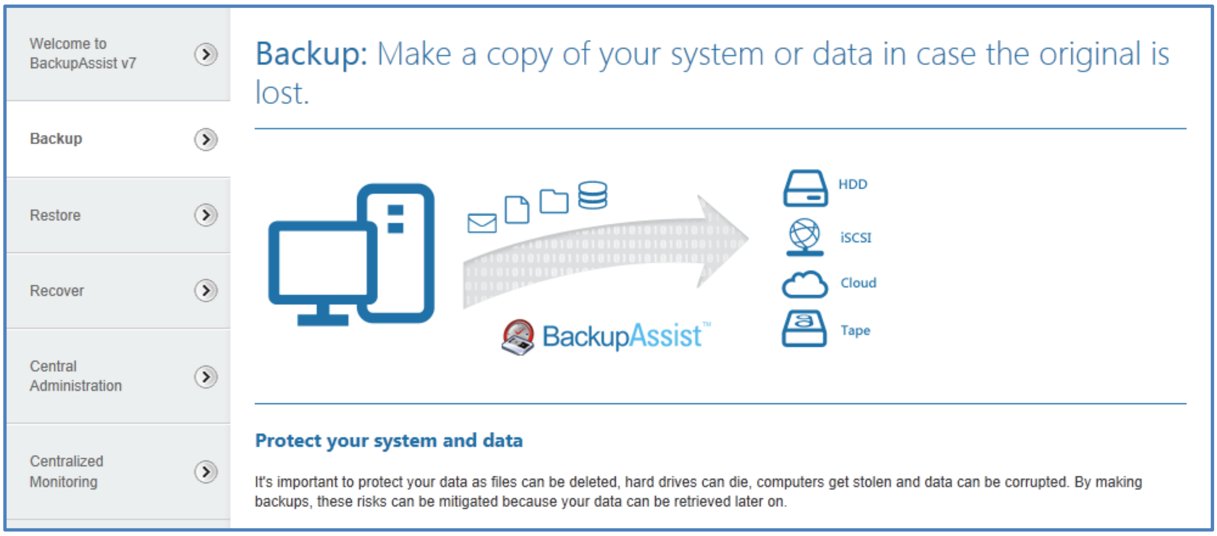
Should you have any questions regarding either BackupAssist or System Protection, please email support@backupassist.com and we will respond to you as soon as possible.

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

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.



Backup: Make a copy of your system or data in case the original is lost.

Protect your system and data

It's important to protect your data as files can be deleted, hard drives can die, computers get stolen and data can be corrupted. By making backups, these risks can be mitigated because your data can be retrieved later on.

Figure 10: Backup tab - Welcome Screen