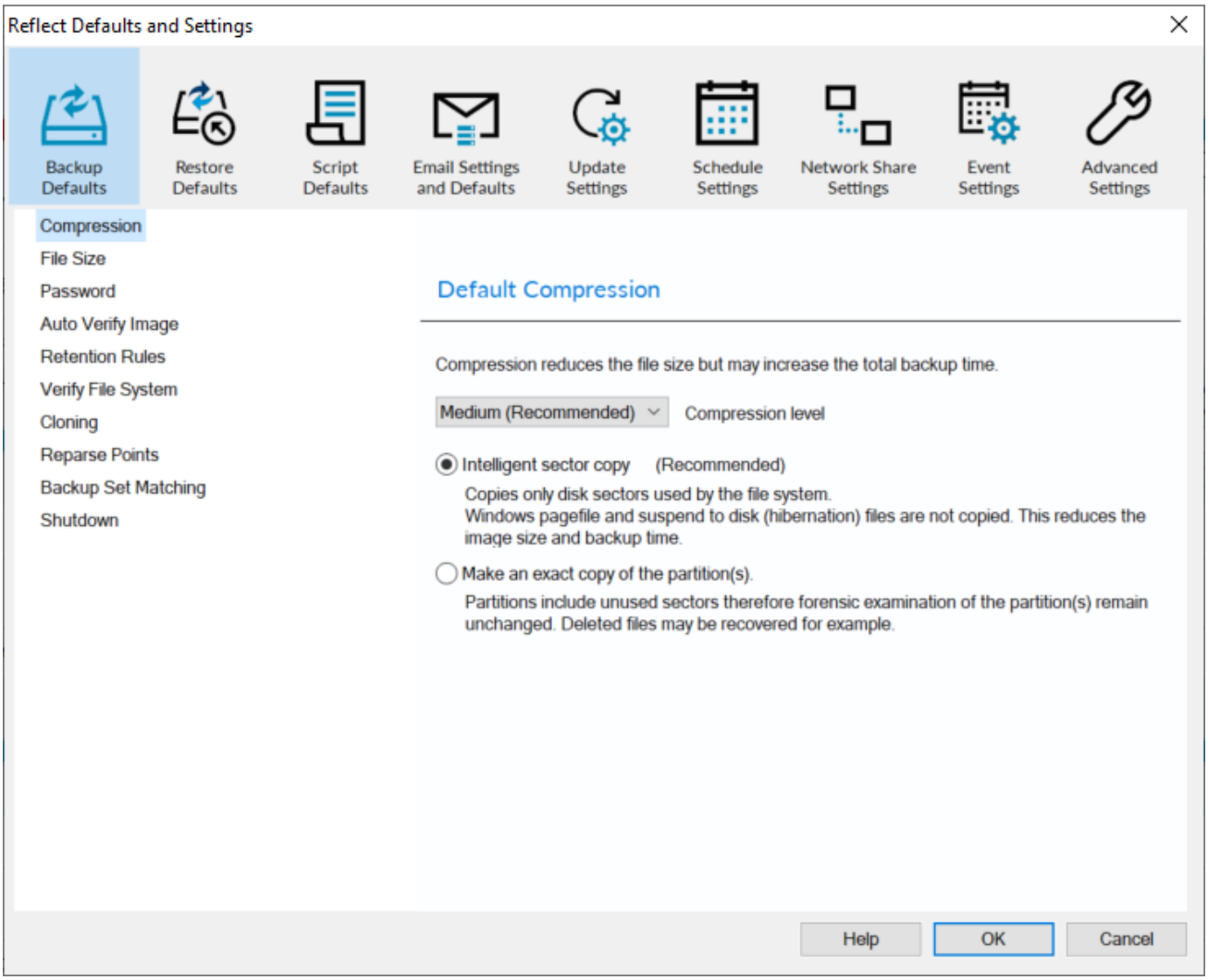
Backup Defaults

Note: New Backup Definitions will use the default values set here. **Existing backups definitions will not be affected.**

Compression



Backup files can be reduced in size without compromising data integrity. Compression results may vary depending on compressibility of the source data, e. g., a standard Windows install OS partition will compress to around 60-70% of its original size. The compression effectiveness for user data partitions and files will depend on the types of files being backed up. Files that won't compress further include most audio and video files, as well as existing compressed file such as .zip, .tar, .7z etc.

Compression Level	Description
None	Backup without compressing.

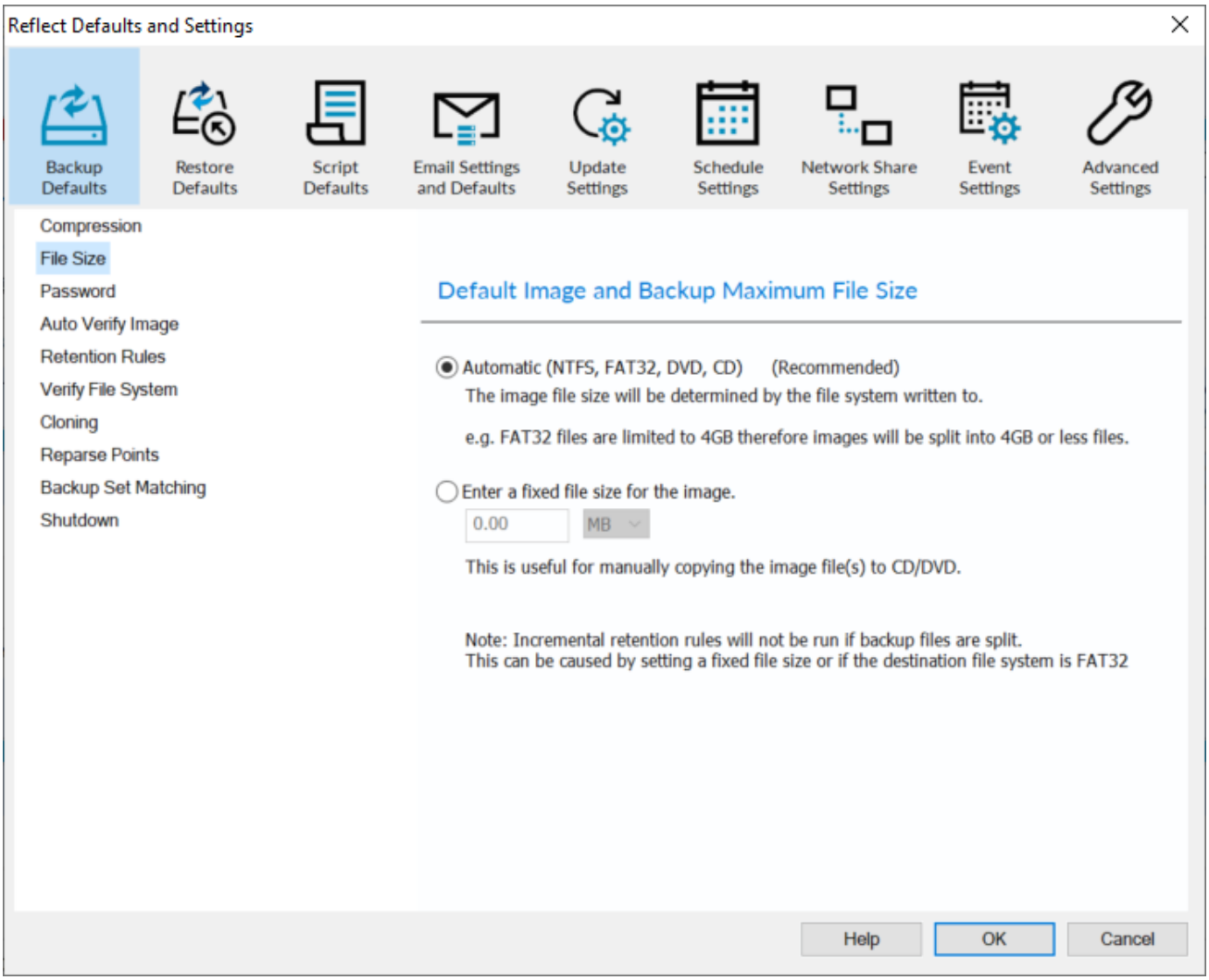
Medium (Recommended)	Medium compression generally provides the best compromise for performance and file size.
High	High compression may make backups take considerably longer to complete but the difference in file size may be marginal.

Macrium Reflect uses a very fast, real-time, *streaming block compression algorithm. This will not provide the same overall compression ratio as common compression utilities such a 7-Zip which use, much slower, whole file data compression techniques.

*All 'mountable' backup files, such as those created by Macrium Reflect, require discrete blocks of data to be compressed and decompressed 'on the fly'. This enables images and backup files to be incremented and mounted as drives in Windows Explorer,

Option	Description
Intelligent Sector Copy	Only backup data blocks that are being used by files on the disk. This significantly reduces the time it takes for backups to complete and reduces the size of the backup files. The data blocks in Pagefile (pagefile.sys) and hibernation (hiberfil.sys) files will be excluded from images. Data blocks in these files are temporary and not required when Windows starts. These files will be visible in the imaged file system, but will take up zero space in the image file.
Forensic Copy	Backup all data blocks. This may significantly increase the size of image files. e.g., An image of a 1TB file system with only 1GB in use will contain 1TB of data blocks prior to any compression.

File Size

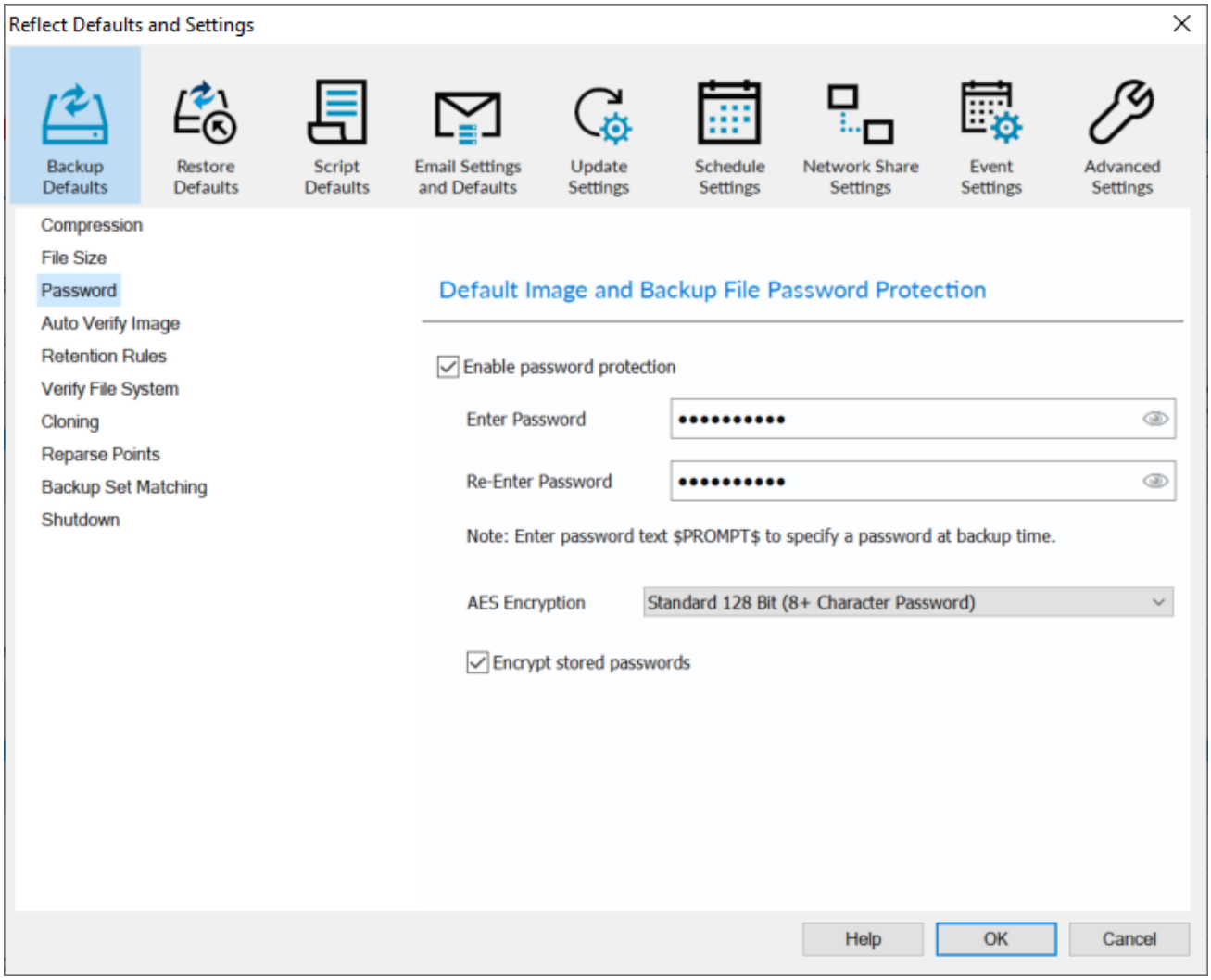


Incremental Retention Rules will not be run if backup files are split. This can be caused by setting a fixed size or if the destination file system is FAT32.

Option	Description

Automatic (Recommended)	Let the system decide on how large the images are going to be created dependent on file system (NTFS, FAT32, DVD, CD) e.g. FAT32 files are limited to 4GB therefore images are going to be split into 4GB or less files.
Fixed file size	Create Images that will be split into many fixed size files. This is useful when copying Image files to optical media or to some cloud storage providers.

Password

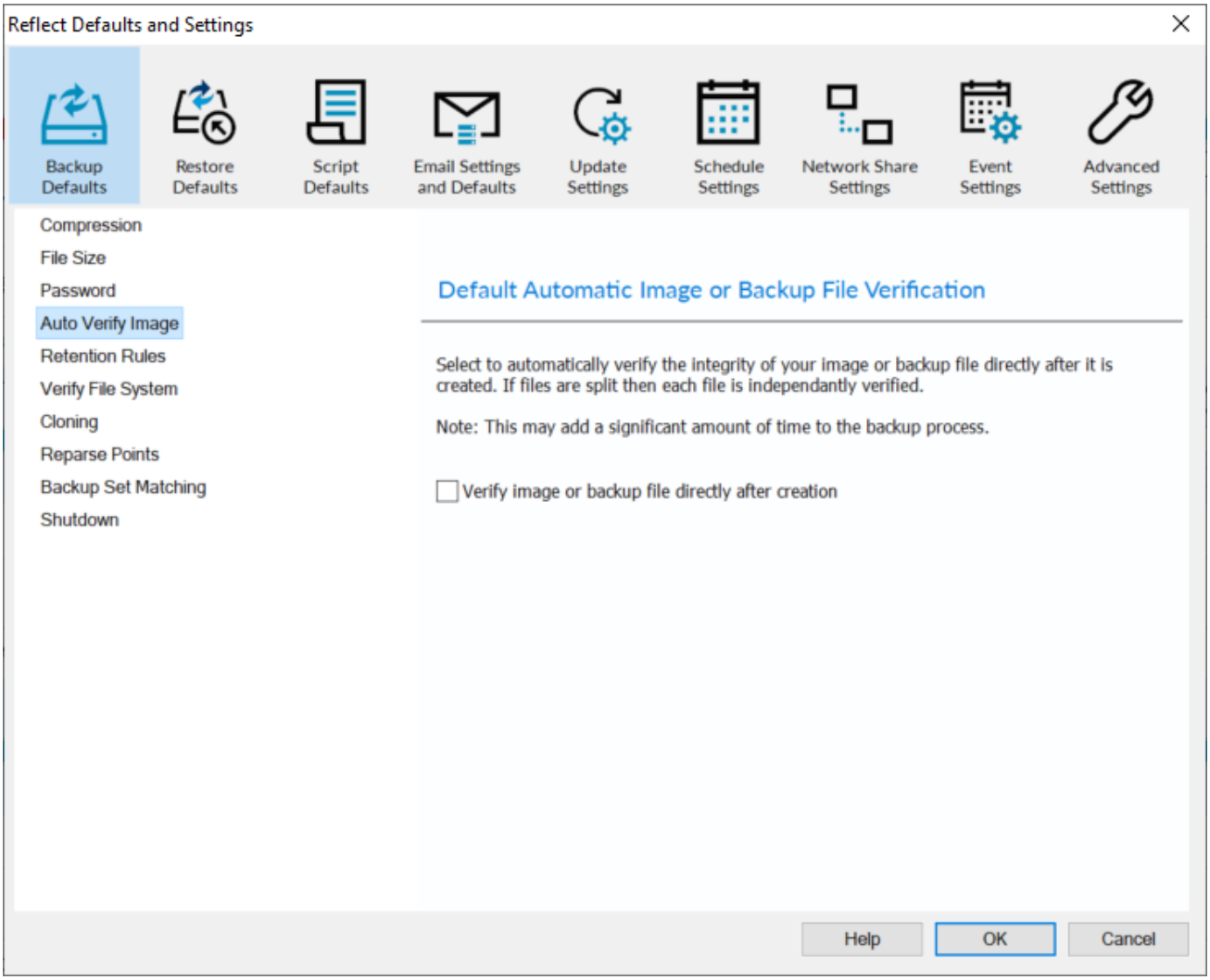


With the **Password** option turned on all the images created will require a password before they can be browsed or restored.

Enter Password:	The minimum password length is determined by the selected AES encryption level. Long passwords are much more secure than shorter passwords and can easily be constructed and remembered by adding together phrases and words that are unique to your memory. Passwords are not saved to backup files. Macrium Reflect uses standard PBKDF2 key derivation functions with 260K iterations to save an irreversible hash of the password. To **view existing** saved **passwords**, **click the 'eye' icon** in the password edit field. After entering valid Windows Administrator credentials, the password will be shown in plain text.
AES Encryption	

None	No encryption and the password can be any length.
Standard 128 Bit	This is the default and requires a password containing at least 8 characters.
Medium 192 Bit	Requires a password containing at least 16 characters.
High 256 Bit	Requires a password containing at least 32 characters.
Encrypt stored passwords	Passwords are stored in backup definition files to enable unattended backups to run. Select this option to encrypt your passwords in the xml file using a steganographically hidden asymmetric key. To prevent unauthorized access we recommend that backup definition files are saved to a secure location on your file system. If having a reversible encrypted password saved on your system presents an unacceptable security risk then **enter the password $PROMPT$ in the password field**. Once typed, the letters become visible and running backup definitions with this password will enforce manually creating and enter a password whenever the backup is run. Please note that it will not be possible to schedule unattended backups in this case: 

Auto Verify Image

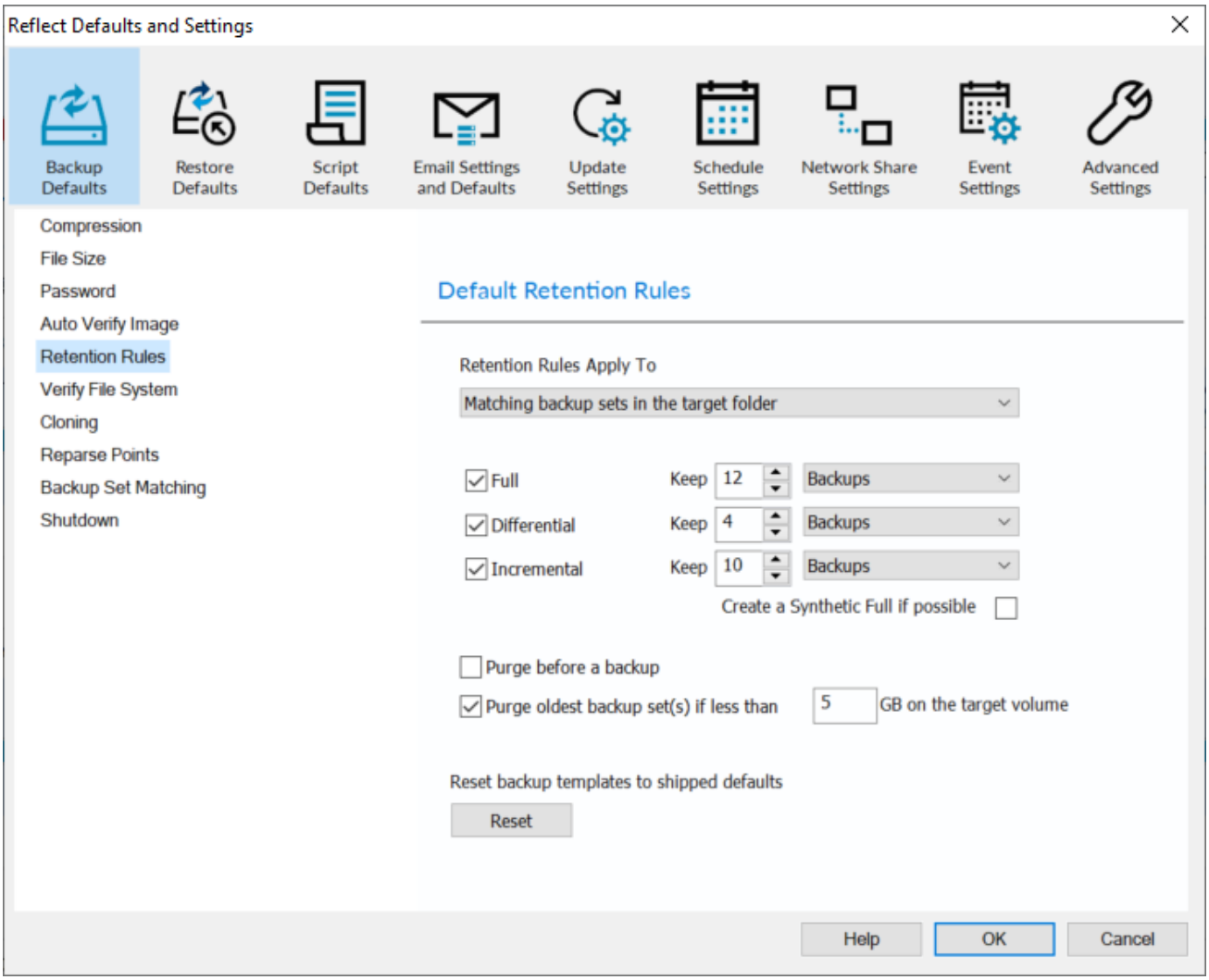


Option	Description
Verify image	Images will be verified automatically when the backup completes. **Note:** This can add a significant amount of time to the backup process.

For more information on image verification please see Understanding Image Verification Failures

---

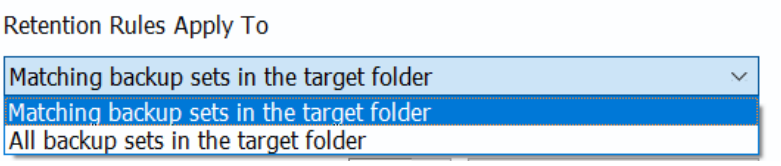
Retention Rules



Macrium Reflect retention rules provide a powerful and flexible way to manage the lifetime and storage space used by your backups.

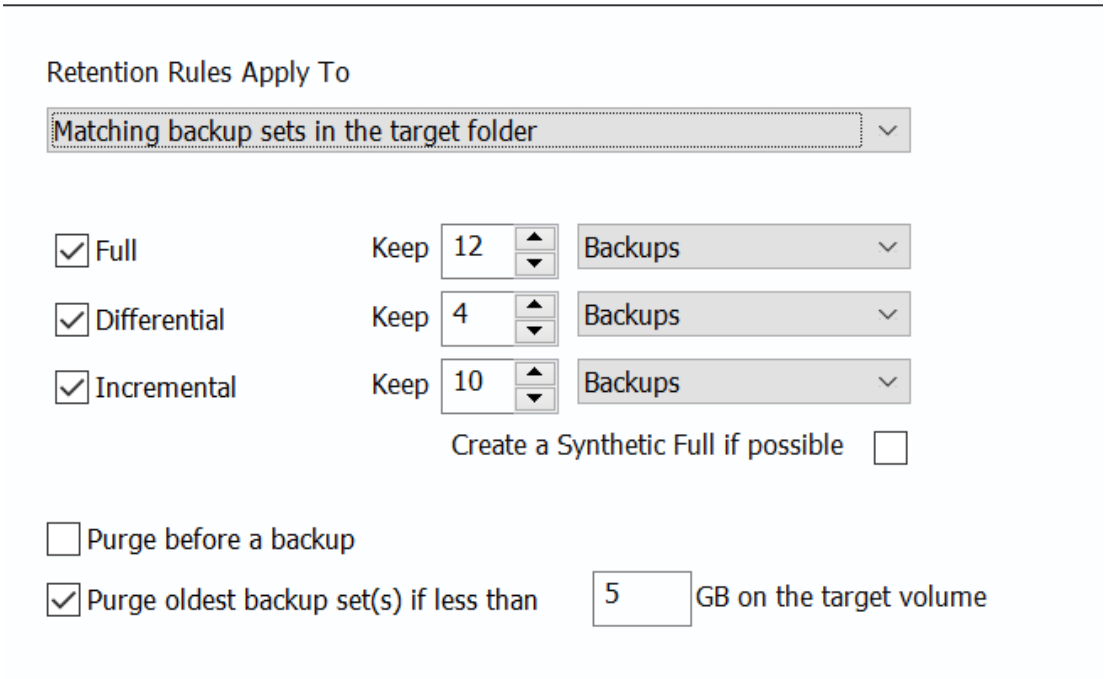
Choose how backups are matched, and how retention rules are applied to the target folder

Retention rules are applied to the target folder of the backup by selecting one of two options:



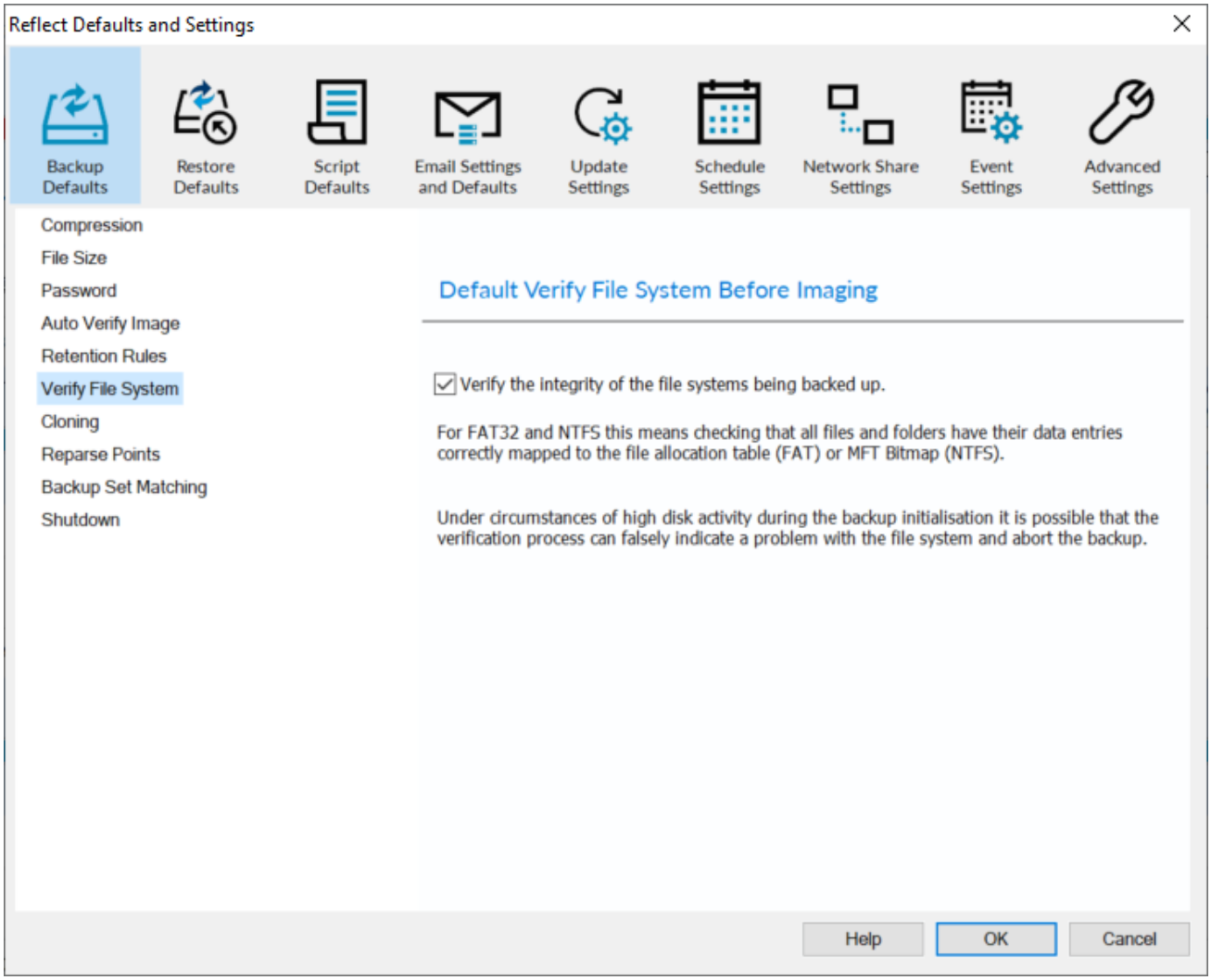
Similar backup sets in the target folder.	**Disk Images** are purged if they contain **exactly the same Partitions** as the current Image. Partitions are identified using the unique **Disk ID** stored in sector 0 of the disk and the **Partition sector offset**. **Note:** For GPT disks the unique GPT disk GUID is used instead of the Disk ID For **File and Folder** backups retention rules are applied according to the File and Folder '**Backup Set Matching'** selection.
All backup sets in the target folder.	All backup sets in the target folder of the same type (Disk Image or File and Folder) are purged according the retention rules.

Select the age or number of backup types that you wish to keep



Option	Description
Full	When deleting Full backups all linked incremental and Differential backups in the same backup chain (set) are also deleted This operation will delete the entire backup set.
Differential	When deleting Differential backups all linked incremental backups in the same backup chain (set) are also deleted.
Incremental	When deleting Incremental backups the integrity of the backup set is maintained by ensuring that the chain is never broken. This is achieved by merging older Incremental backups when required. In the example below, before retention, there is **1 Full backup, 1 Differential backup** and **6 Incremental** backups. The retention rules are set to **retain 4 incremental** backups. After retention, the most recent 4 incremental backups are retained. **Deleting the oldest 2 incrementals would cause the backup chain to be invalid** as the oldest retained incremental requires the previous 2 incremental backups to complete the chain. To ensure backup integrity the **2 older incremental backups are consolidated** with it to create a new incremental backup. **F = Full** **D = Differential** **I = Incremental** M T W T F M T W T F M T W F D I I I I I F I I -- -> I
Create a Synthetic Full if possible	When purging Incremental backups, if the backup set **only contains a Full backup followed by Incremental backups**, then this option causes the Full backup to be 'rolled forward' to **create a Synthetic Full backup**. This is also known as **Incremental Forever.**
Run the purge before the backup	Select this option to run the retention rules before the current backup. **Note:** in Macrium Reflect v5 the current backup set wasn't included in the purge calculation when purging before the current backup. In v6 the current backup set **IS** included. This means that if you set the retention count to 1 Full backup then all of your backups will be deleted and a new Full backup created.
Delete oldest backup set(s) if less than n GB	Automatically remove the oldest backup set(s) in the target folder if the free space on the drive drops below the GB threshold. **Note:** The free space threshold is actioned dynamically. If the free space available drops below the threshold then the running backup is temporarily paused while older backup sets are purged.

Verify File System

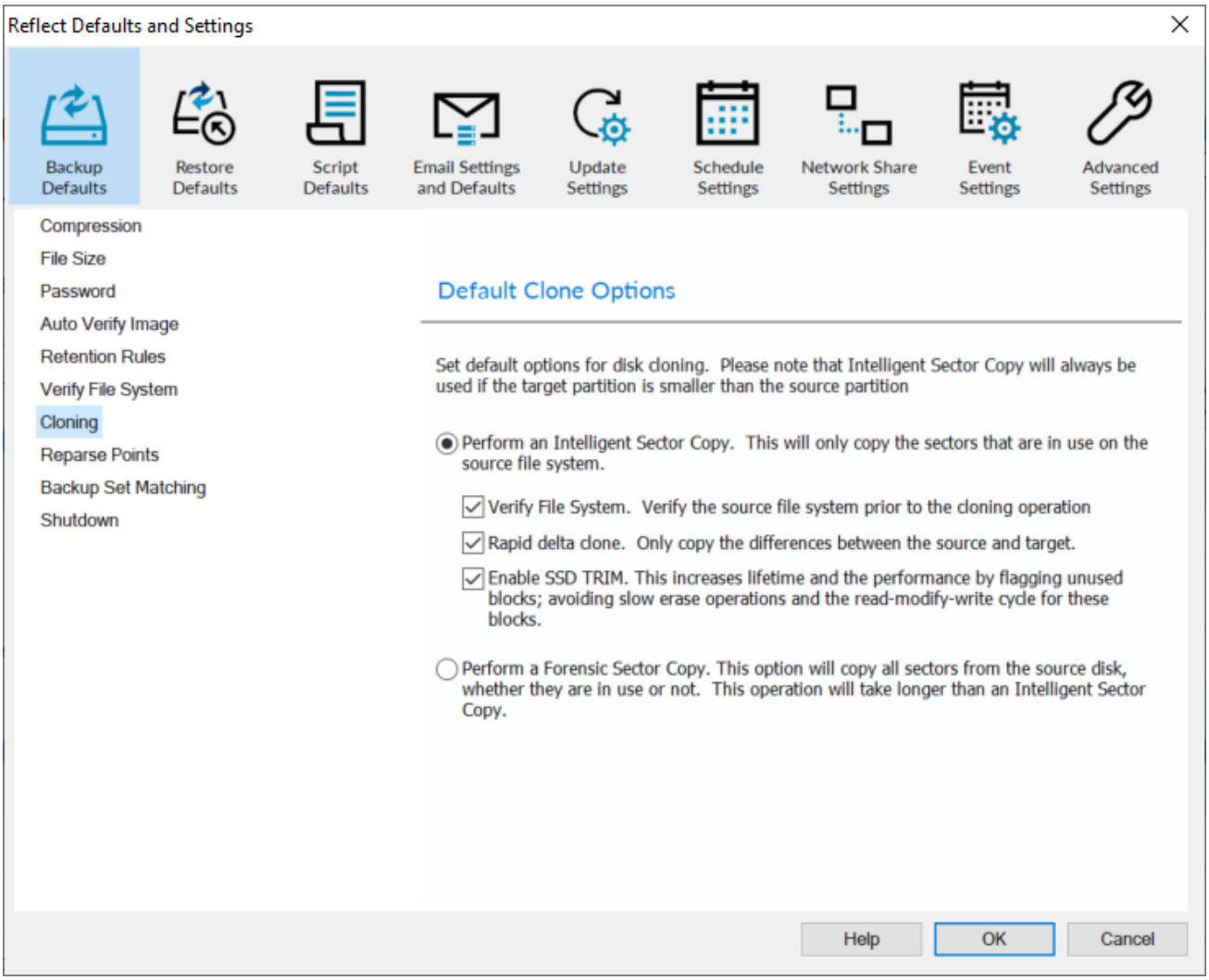


Verify File System is used to check the integrity of the file system before a backup.

Macrium Reflect will automatically verify the integrity of FAT32 and NTFS file systems being backed up. This means checking that all files and folders have their data entries correctly mapped to the file allocation table (FAT) or $MFT Bitmap (NTFS).

This is a comprehensive check, and similar in functionality to the MS-DOS chkdsk command that may increase the time taken to complete a backup.

Cloning



Option	Description

<table>
<tr><td>Perform an Intelligent Sector Copy</td><td>Only backup the sectors that are being used by data on the disk. Pagefile (pagefile.sys) and hibernation (hiberfil.sys) will be excluded.

This reduces the time it takes for the clone to complete.

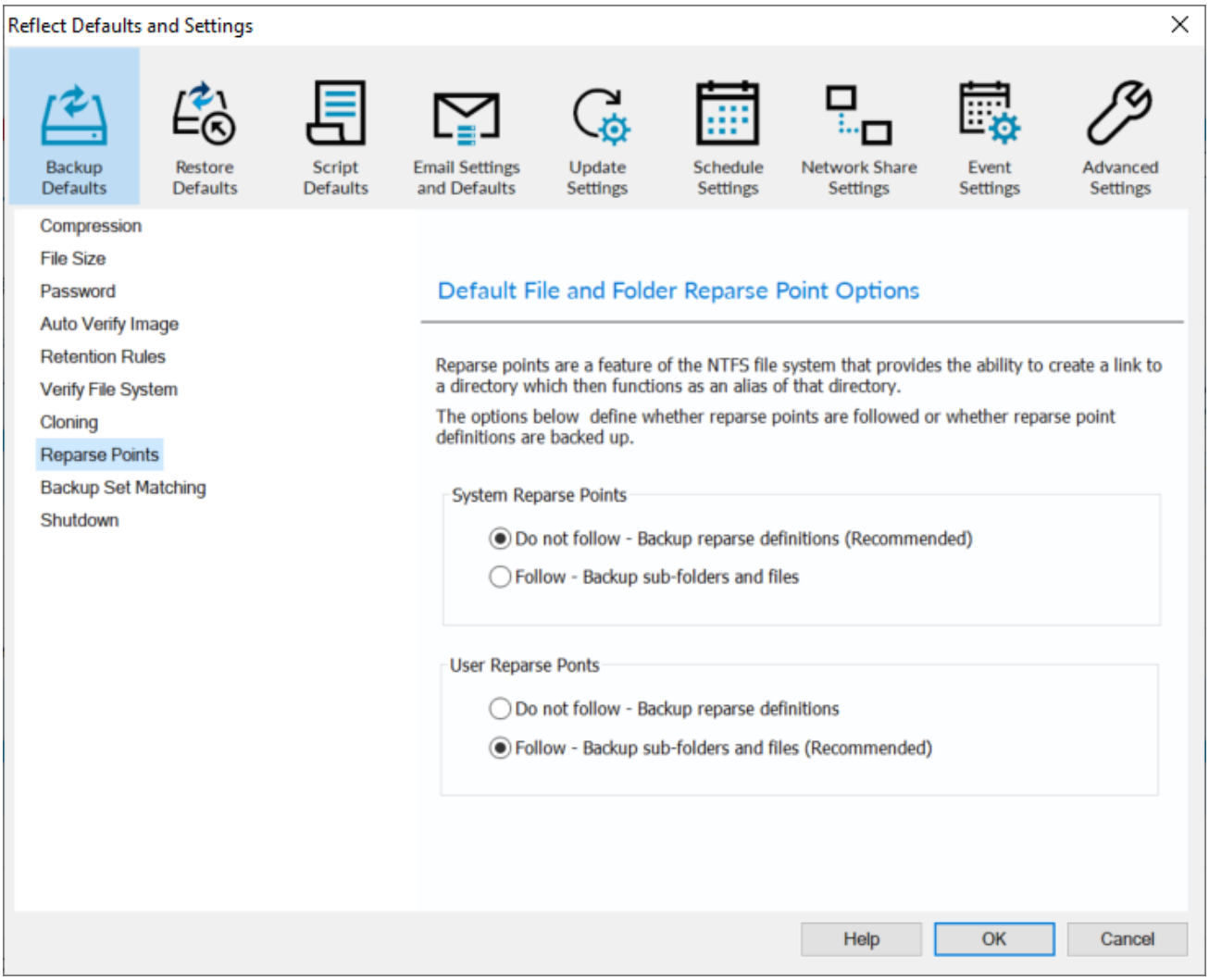
<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Verify File System</td><td>Reflect will verify the integrity of your file system; Verification check that all files and folders data entries are correctly mapped to the file allocation table (FAT) or MFT Bitmap (NTFS)</td></tr>
<tr><td>Rapid Delta Clone</td><td>As with Rapid Delta Restore (RDR) the concept of RDR has been something that has been thought about for quite some time here at Macrium Software. We wanted to build a clone solution that would effectively and rapidly copy only the differences between the source and target file systems. The advantage of this is obvious, RDC offers similar a performance increase as an Incremental disk image offers over a Full image and enables regular clones to be a viable and fast DR solution.

How does it work?

The NTFS file system resident on the clone source is compared with file system on the target disk. The two file systems are first verified that they originated from the same format command and then the target NTFS file system structures are analyzed for differences. All the NTFS file system structures are copied to the target disk and any that do not exist or have been modified on the target disk cause the data records for each NTFS file or object to be copied as well. The result is an 'Incremental' clone applying only file system changes detected between the source and the target.
Note: RDC works with NTFS file systems only. All other file systems will perform a full clone
Note: RDC is not available when shrinking partitions during a clone.</td></tr>
<tr><td>Enable SSD TRIM</td><td>This features provides automated SSD optimization resulting enhanced SSD performance and longevity. Writing to an unused block is much quicker than an in-use block as it avoids both the slow erase operation and the read-modify-write cycle. This results an increase of both the lifetime and the performance of the device. It is effective for all windows operating systems, even those that support SSD trim natively as the file system driver can only TRIM blocks on de-allocation; it cannot TRIM blocks written by another process. It is also effective for USB attached SSDs.</td></tr>
</table>
</td></tr>
<tr><td>Perform a Forensic Sector Copy</td><td>Backup every sector.

This can add a significant amount of time to the backup process.</td></tr>
</table>

Reparse Points



Reparse points are a feature of the NTFS file system that provides the ability to create a link to a directories which then fictions as an alias of that directory.

e.g. Reparse point is the folder "Documents and Settings" which when followed points (or expands) to a number of other folders. If followed then all folders the reparse point "contents" will be included in the backup.

The options below define whether reparse points are followed or whether reparse point definitions are backed up.

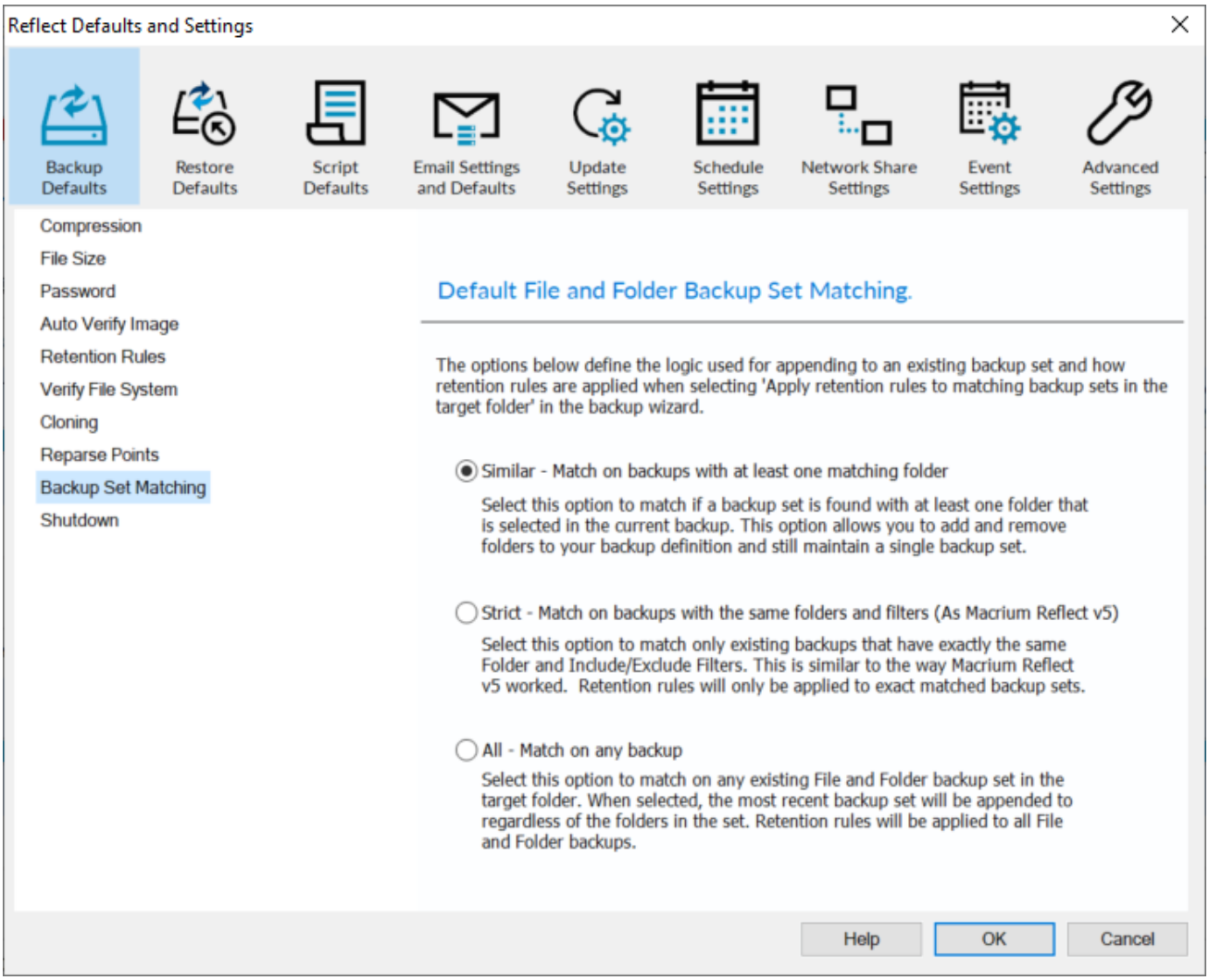
Reparse points are defined by folder attributes, and **all** reparse point tags are considered.
See: https://docs.microsoft.com/en-us/windows/win32/fileio/reparse-point-tags

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>System Reparse Points</td><td>Attributes
FILE_ATTRIBUTE_DIRECTORY | FILE_ATTRIBUTE_REPARSE_POINT | FILE_ATTRIBUTE_SYSTEM

<table><tr><td>Do not follow</td><td>Only backup the Reparse Definitions (Recommended)</td></tr><tr><td>Follow</td><td>Backup all the Reparse Points</td></tr></table></td></tr>
<tr><td>User Reparse Points</td><td>Attributes
FILE_ATTRIBUTE_DIRECTORY | FILE_ATTRIBUTE_REPARSE_POINT

<table><tr><td>Do not follow</td><td>Backup the Reparse Definitions</td></tr><tr><td>Follow</td><td>Backup all the Reparse Points (Recommended)</td></tr></table></td></tr>
</table>

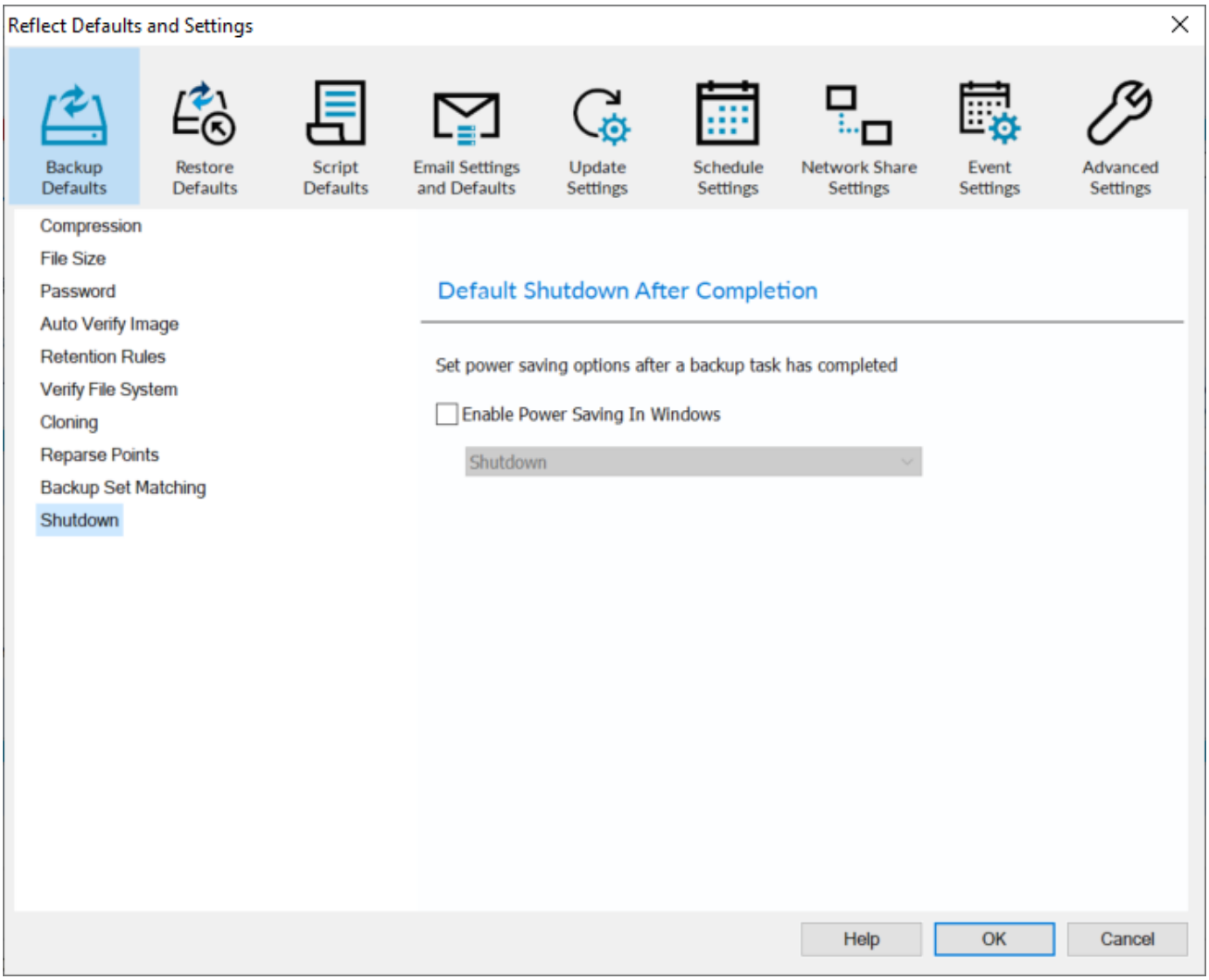
Backup Set Matching



The options below define the logic used for appending to an existing backup set and how retention rules are applied when selecting **'Apply retention rules to matching backup sets in the target folder'** in the backup wizard.

Option	Description
Similar - Match on backups with at least one matching folder	Add and remove folders in your backup definition and still maintain a single backup set.
Strict - Match on backups with the same folders and filters	Retention rules will only be applied to exact matched backup sets.
All - Matching on any backup	Retention rules will be applied to all File and Folder backup sets.

Shutdown



Option	Description
Shutdown	This will **Shutdown** your computer after the backup is complete. A sub-option can be enabled to **Force the shutdown process** - All programs will be forced to close without being queried.
Hibernate	This will **Hibernate** your computer after the backup is complete
Suspend	This will put your computer to **Sleep** after the backup is complete.