# **Backup Defaults**

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

- Compression
- File Size
- Password
- Auto Verify Image
- Retention Rules
- Verify File System
- Cloning
- Reparse Points
- Backup Set Matching
- Shutdown

## Compression

Reflect Defaults	and Settings							×
Backup Defaults	Restore Defaults	Script Defaults	Email Settings and Defaults	Update Settings	Schedule Settings	Network Share Settings	Event Settings	Advanced Settings
Compression File Size Password Auto Verify Im	nage		Default C	ompression	1			
Retention Rules       Compression reduces the file size but may increase the total backup time.         Verify File System       Medium (Recommended) ~ Compression level         Cloning       Medium (Recommended) ~ Compression level         Reparse Points       Intelligent sector copy (Recommended)         Backup Set Matching       Copies only disk sectors used by the file system.         Windows pagefile and suspend to disk (hibernation) files are not copied. This reduces the image size and backup time.						reduces the		
			Partitions unchange	include unused d. Deleted files	sectors therefor may be recovere	e forensic examinat ad for example.	ion of the partit	ion(s) remain
						Help	ОК	Cancel

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	Let the system decide on how large the images are going to be created dependent on file system (NTFS, FAT32, DVD, CD)
(Recommended)	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

Reflect Defaults	and Settings							×
Backup Defaults	Restore Defaults	Script Defaults	Email Settings and Defaults	Update Settings	Schedule Settings	Network Share Settings	Event Settings	Advanced Settings
Compression File Size Password	nade		Default Im	nage and B	ackup File Pa	assword Protect	ction	
Retention Ru	iles stem		C Enable pas	sword protecti	on			
Cloning			Enter Pass	sword	•••••			٢
Reparse Poir	nts		Po-Entor [	accuord				
Backup Set I Shutdown	Matching		Re-Enter Password					
Childonn			Note: Ente	er password te	kt \$PROMPT\$ to	specify a password	at backup time.	
			AES Encry	ption S	tandard 128 Bit (	8+ Character Passv	vord)	~
			Encryp	t stored passw	ords			
						Help	OK	Cancel

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

Enter Passw ord:	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 Encryp tion							

None	No encryption and the password can be any length.								
Standa rd 128 Bit	This is the default and requires a password containing at least 8 characters.								
Mediu m 192 Bit	Requires a password containing at least 16 characters.								
High 256 Bit	Requires a password containing at least 32 characters.								
Encryp t stored passw ords	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 <b>enter the password</b> <b>\$PROMPT\$ in the password field</b> . 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: <b>Enter Password protection</b> <b>Enter Password \$PROMPT\$</b>								

## Auto Verify Image

Reflect Defaults	and Settings							×
Backup Defaults	Restore	Script Defaults	Email Settings and Defaults	Update Settings	Schedule	Network Share Settings	Event Settings	Advanced Settings
Compression File Size Password Auto Verify II Retention Ru Verify File Sy Cloning Reparse Poil Backup Set	nage ules stem nts		Default Au Select to autor created. If file Note: This ma	matically verify s are split then ay add a signific	the integrity of y each file is indep ant amount of ti	your Image or backup nour Image or backup pendantly verified. me to the backup p	p file directly a	ifter it is
Backup Set Matching Verify image or backup file directly after creation								
						Help	ОК	Cancel

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**

Reflect Defaults and Settings				×
Backup Defaults Backup	Email Settings Update Settings	Schedule Settings	re Event A Settings S	dvanced Settings
Compression File Size Password Auto Verify Image	Default Retention Rules			
Retention Rules Verify File System Cloning Reparse Points Backup Set Matching	Retention Rules Apply To Matching backup sets in the ta	rget folder ep 12 🖕 Backups	~	
Shutdown	<ul><li>✓ Differential Kee</li><li>✓ Incremental Kee</li></ul>	p 4 Backups p 10 Backups Create a Synthetic Full	if possible	
	Purge before a backup Purge oldest backup set(s) Reset backup templates to shipp Percet	if less than 5 GB red defaults	on the target volume	
	iveset	Help	ОК	Cancel

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:

Retention Rules Apply To

Matching backup sets in the target folder	~
Matching backup sets in the target folder	
All backup sets in the target folder	

Similar backup sets in the target folder.	<ul> <li>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</li> <li>For File and Folder backups retention rules are applied according to the File and Folder 'Backup Set Matching' selection.</li> </ul>
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

Reten	tion Rules Apply To							
Match	ning backup sets in t	ne targ	et fold	er	$\sim$			
						a		
🗸 Fi	ull	Кеер	12	▲ ▼	Backups ~			
VD	ifferential	Кеер	4	▲ ▼	Backups ~			
✓ Ir	ncremental	Кеер	10	▲ ▼	Backups 💉			
			Creat	e a S	Synthetic Full if possible			
☐ Pu ✓ Pu	irge before a backup irge oldest backup se	et(s) if l	ess th	an	5 GB on the target v	volume		
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	cremental       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							

Incremental	When de	eleting Inc	remental	backups t	the integri	ty of the b	backup se	t is maint	ained by	ensuring	that the ch	nain is ne	ver broke	n. This is	achieved	by mergir	ng older I	Incremental backups when required.	
	In the ex most rec incremen	In the example below, before retention, there is <b>1 Full backup</b> , <b>1 Differential backup</b> and <b>6 incremental</b> backups. The retention rules are set to retain <b>4 incremental</b> backups. After retention, the most recent <b>4</b> incremental backups are retained. <b>Deleting the oldest 2 incrementals would cause the backup chain to be invalid</b> as the oldest retained incremental requires the previous 2 incremental backups to complete the chain. To ensure backup integrity the <b>2 older incremental backups are consolidated</b> with it to create a new incremental backup.																	
	F = Full D = Diffe I = Incre	erential emental																	
	м	т	w	т	P			м	т	w	т	P			м	т	w		
	F							D	I	I	I	I			F	I	I	-	
									-	->	I								
Create a Synthetic Full if possible	When pu Synthet	urging Incr ic Full ba	emental t ckup. Thi	oackups, s is also l	if the bacl known as	kup set or Increme	nly conta ntal Fore	ins a Ful ver.	l backup	followed	by Incre	mental b	ackups, t	hen this o	ption cau	ses the F	ull backu	p to be 'rolled forward' to <b>create a</b>	
Run the purge before the backup	<ul> <li>Select this option to run the retention rules before the current backup.</li> <li>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.</li> </ul>																		
Delete oldest backup set(s) if less than n GB	Automat Note: Th	ically remo ne free spa	ove the ol ace thresh	dest back nold is act	kup set(s) tioned dyr	in the tar namically.	get folder If the free	if the free e space a	e space o vailable d	n the driv Irops belo	e drops be w the thre	elow the C eshold the	GB thresh In the run	old. ning back	up is tem	porarily p	aused wh	nile 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

Reflect Defaults	s and Settings							×
Backup Defaults	Restore Defaults	Script Defaults	Email Settings and Defaults	Update Settings	Schedule Settings	Network Share Settings	Event Settings	Advanced Settings
Compression File Size Password Auto Verify II Retention Re Verify File Sy Cloning Reparse Poil Backup Set I Shutdown	n mage ules rstem nts Matching		Default Cl Set default op used if the tar Perform ar source file Verify F Rapid c Enable blocks; blocks. Perform a whether th Copy.	lone Option tions for disk d get partition is n Intelligent See system. File System. Ve delta clone. On SSD TRIM. Thi avoiding slow Forensic Sector ley are in use o	IS Ioning. Please n smaller than the tor Copy. This rify the source f ly copy the diffe s increases lifeti erase operations Copy. This opti r not. This oper	ote that Intelligent : source partition will only copy the s ile system prior to t rences between the me and the perform and the read-modi on will copy all sect ation will take long	Sector Copy wil ectors that are i he cloning oper source and targ iance by flaggin fy-write cycle fo tors from the so er than an Intel	I always be n use on the ation get. g unused or these urce disk, ligent Sector
						Help	ОК	Cancel
Option De	escription							

Perform an Intellige	Only backup This reduce	o the sectors that are being used by data on the disk. Pagefile (pagefile.sys) and hibernation (hiberfil.sys) will be excluded. s the time it takes for the clone to complete.						
Sector Copy	Option	Description						
	Verify File System	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)						
	Rapid Delta Clone	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. <b>Note:</b> RDC works with NTFS file systems only. All other file systems will perform a full clone <b>Note:</b> RDC is not available when shrinking partitions during a clone.						
	Enable SSD TRIM	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.						
Perform a Forensic Sector Copy	Backup eve This can ad	ry sector. d a significant amount of time to the backup process.						

## **Reparse Points**

Reflect Defaults	and Settings							×
Backup Defaults	Restore Defaults	Script Defaults	Email Settings and Defaults	Update Settings	Schedule Settings	Network Share Settings	Event Settings	Advanced Settings
File Size Password Auto Verify II	nage		Default Fi	le and Fold	er Reparse P	oint Options		
Retention R	ules		Reparse point a directory wh	s are a feature hich then function	of the NTFS file s ons as an alias of	system that provide that directory.	s the ability to	create a link to
Cloning	Stom		The options b definitions are	elow define wi	hether reparse po	pints are followed o	r whether repa	rse point
Reparse Poir	nts							
Backup Set	Matching		System Rep	arse Points				
Shutdown			Do	not follow - Ba	ckup reparse defi	initions (Recommen	ded)	
			◯ Foll	ow - Backup su	b-folders and file	25		
			User Repars	e Ponts				
			ODo	not follow - Ba	ckup reparse defi	nitions		
			Foll	low - Backup su	b-folders and file	es (Recommended)		
						Help	OK	Cancel

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

Option	Description								
System Reparse Points	Attributes FILE_ATTRIBUT	Attributes FILE_ATTRIBUTE_DIRECTORY   FILE_ATTRIBUTE_REPARSE_POINT   FILE_ATTRIBUTE_SYSTEM							
	Do not follow	Do not follow Only backup the Reparse Definitions (Recommended)							
	Follow Backup all the Reparse Points								
User Reparse Points	Attributes FILE_ATTRIBUTE_DIRECTORY   FILE_ATTRIBUTE_REPARSE_POINT								
	Do not follow	Do not follow Backup the Reparse Definitions							
	Follow	Backup all the Reparse Points (Recommended)							

## Backup Set Matching

Reflect Defaults	and Settings							×
Backup Defaults	Restore Defaults	Script Defaults	Email Settings and Defaults	Update Settings	Schedule Settings	Network Share Settings	Event Settings	Advanced Settings
Compression File Size Password	nade		Default Fi	ile and Fold	er Backup Se	et Matching.		
Retention Ru Verify File Sy Cloning Reparse Poir Backup Set I Shutdown	nage stem nts Matching		The options b retention rule target folder Similar Select th is select folders	below define the s are applied wi in the backup w - Match on back his option to ma ted in the current to your backup	logic used for a hen selecting 'Ap izard. cups with at least atch if a backup s t backup. This o definition and sti	ppending to an exis ply retention rules t cone matching fold set is found with at ption allows you to ill maintain a single	ting backup sel to matching bac er least one folder add and remov backup set.	t and how ckup sets in the that ve
			<ul> <li>Strict - I</li> <li>Select ti</li> <li>Folder a v5 work</li> <li>All - Ma</li> <li>Select ti</li> <li>target fr</li> <li>regardle</li> <li>and Folder</li> </ul>	Match on backu his option to ma and Include/Exc ced. Retention atch on any back his option to ma older. When sel ess of the folder der backups.	ps with the same atch only existing lude Filters. This rules will only be cup atch on any existi ected, the most r s in the set. Rete	e folders and filters backups that have is similar to the wa applied to exact m ing File and Folder recent backup set w ention rules will be a	(As Macrium Re exactly the san by Macrium Refl atched backup backup set in th ill be appended applied to all Fi	effect v5) ne ect sets. ne to le
						Help	ОК	Cancel

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

Reflect Default	s and Settings							×
Backup Defaults	Restore Defaults	Script Defaults	Email Settings and Defaults	Update Settings	Schedule	Network Share Settings	Event Settings	Advanced Settings
Compression File Size Password Auto Verify I	mage		Default SI	hutdown Af	ter Complet	ion		
Retention R Verify File Sy Cloning Reparse Poi	ules /stem		Set power sav	ving options afte wer Saving In V	er a backup task Vindows	has completed		
Backup Set	Matching		Shutdown	n		V		
						Help	OK	Cancel

Option	Description
Shutdown	This will <b>Shutdown</b> 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 <b>Sleep</b> after the backup is complete.