Macrium Image Guardian

Macrium Image Guardian Overview

Macrium Image Guardian protects your backup files from unauthorised modification.

MIG grants write access to existing backups file for Macrium Reflect 7.1, any image tools created by us, and optionally, MS RoboCopy. All other process attempting to update existing backup files will be denied access.

MIG protects local **NTFS** volumes and allows Macrium Reflect 7.1 and later to use the protected volume as a shared network resource.

Macrium Image Guardian protection architecture
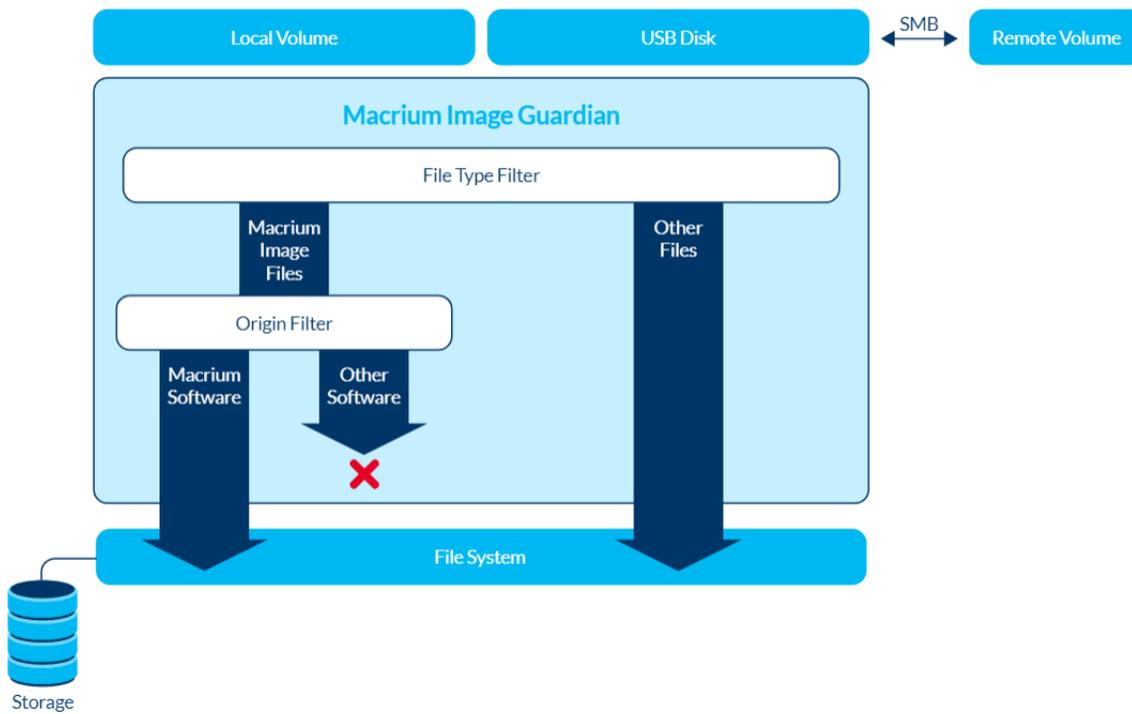
Macrium Image Guardian protecting backups in a networked environment
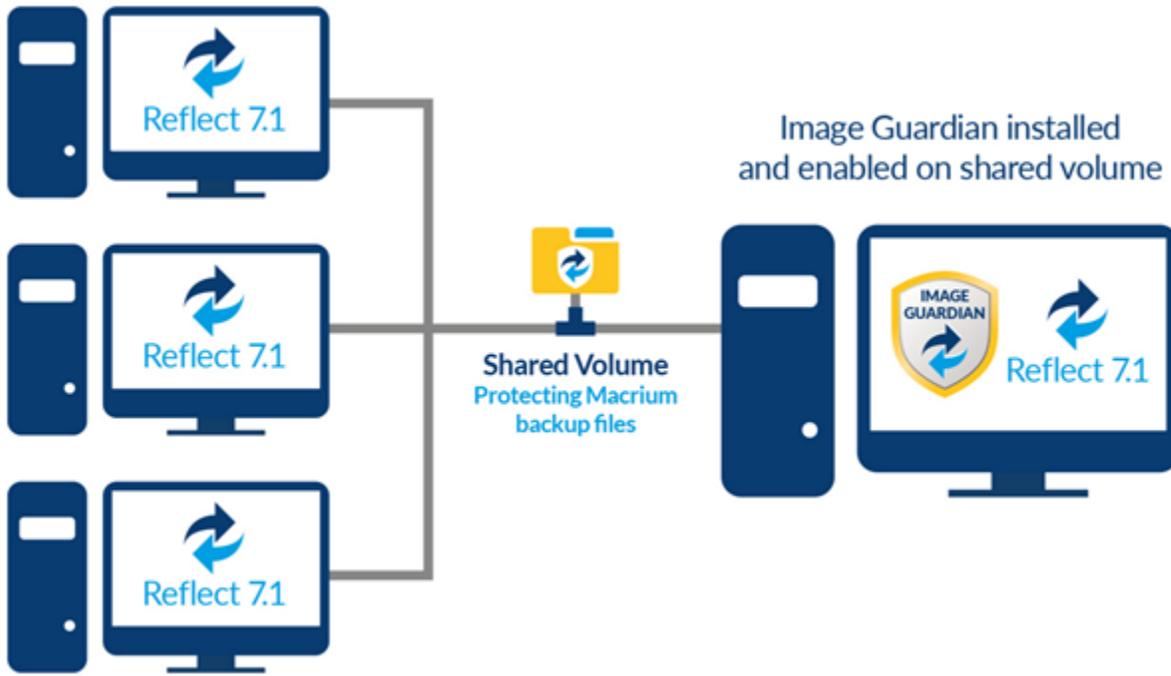
In the above illustration, the PC sharing the backup repository (Shared Volume) has a full install of Macrium Reflect, including **MIG**. A local drive is shared over the network and **MIG** has been enabled on that drive in the Macrium Reflect user interface.

The other PC's on the network can backup to this shared drive and **do not** require MIG to be installed. Backup file write access is automatically granted to Macrium Reflect 7.1, and later, write access for earlier versions of Macrium Reflect and other processes will fail.

The PC hosting the share with **MIG** installed can be used as a standalone Macrium Reflect installation. The protected drive will prevent unauthorised access to backup files on that drive if the local PC creates backups to the protected volume.

Protected File Access

Macrium Image Guardian will protect all existing local backup files from unauthorised modification or deletion. All such activity will be blocked with **error 0x80070510 - Storage policy block**.
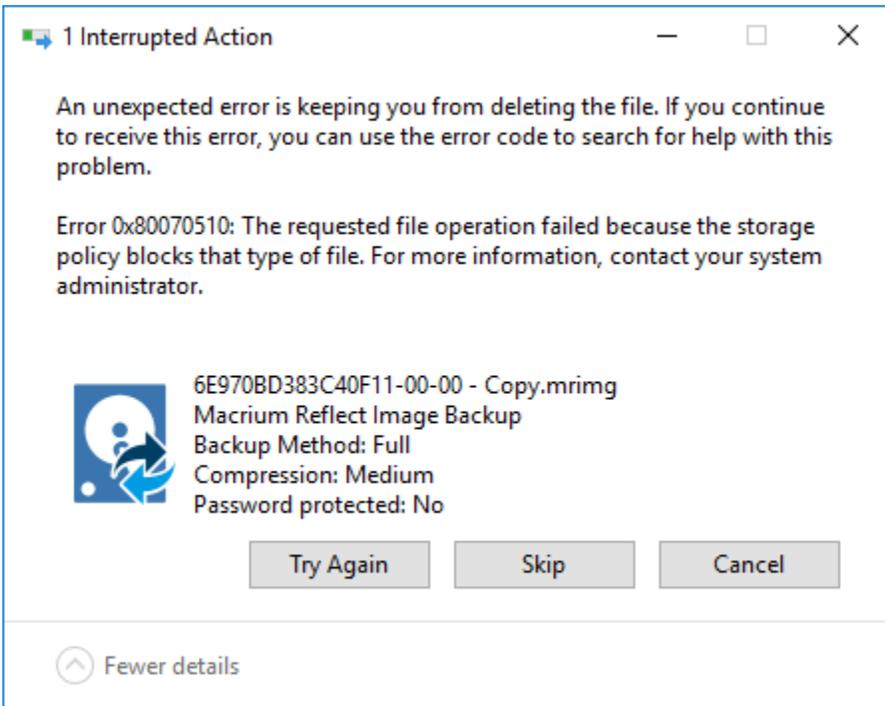
Protected File Types

The following file extensions are protected by Macrium Image Guardian.

Extension	Backup Type
.mrimg	Macrium Reflect image files
.mrbak	Macrium Reflect File and Folder backup files
.mrex	Macrium Reflect Exchange backup files
.mrsql	*Macrium reflect SQL backup files

*Note: SQL backup files can only be created to a protect volume by Macrium Reflect running on the **local PC**. Network write access will be blocked for all processes, including Macrium Reflect. This limitation will be removed in a future update.

Windows File operations on Macrium Backup files

Macrium Image Guardian will block opening of backup files for modification or delete, The following lists some of the operations and special considerations if you are maintaining the location and life of Macrium backup files outside of Macrium Reflect.

1. **Windows Explorer Copy**. New backup files can be created on a protected volume as the result of a **Windows Explorer** copy operation.

    Copying a file to the same folder as the original will be blocked on local file systems. Duplicate files in the same folder is undesirable and should be avoided. The identity of the backup file will be duplicated and this can lead to unpredictable results in Macrium Reflect.

2. **DOS Commands. COPY, MOVE, and XCOPY**. These commands will succeed where the result of the operation is a new file. Overwriting or deleting existing backup files files will fail.

3. **RoboCopy.** RoboCopy.exe can copy, move and synchronise folders. For more information on RoboCopy parameters please see here: https://technet.microsoft.com/en-us/library/cc733145(v=ws.11).aspx

   Some RoboCopy parameters may perform delete file and overwrite operatons on your backup files and have special functionality in MIG if the **'Allow RoboCopy to sync and move backup files on protected volumes'** option is enabled:

| Parameter	Rule
/MOVE /MOV	If the **source folder** is on a protected volume then the **/MOVE /MOV** parameters will only delete backup files in the source folder if the **destination folder is also on a protected volume**. This ensures that existing files cannot be moved to an unprotected volume and compromised.

/MIR /PURGE	If the **target folder** is on a protected volume then the the **/MIR /PURGE** parameters will only delete backup files in the **target folder** if **both** of the following conditions are true:
	
	  a. The source folder **is** a backup destination in any saved backup definition xml file.
	  b. The target folder **is not** a backup destination in any saved backup defintion xml file
	
	This ensures that the synchronisation operation cannot inadvertently, or otherwise, delete files in a folder that is used as a backup destination in Macrium Reflect.

All overwrite operations	If the result of any parameter is to overwrite an existing backup file **on a protected volume** then this will only be allowed if the target folder **is not** a backup destination in any saved backup definition xml file.

RoboCopy and Network Shares

If the **source of a /MOVE /MOV** or **target of a /MIR /PURGE** operation is a **MIG protected volume on a network share** then all delete operations are **blocked.** This is because RoboCopy 'Rules' can only be applied if the Windows session that's opening the files is the same Windows session that's running RoboCopy. In the case of a network share, the remote computer is opening the files and will block all delete operations.

Installing Macrium Image Guardian

MIG is an optional component in the Macrium Reflect installer, It is selected by default and is available for Windows 7 and above in all editions of Macrium Reflect except for the Free Edition.
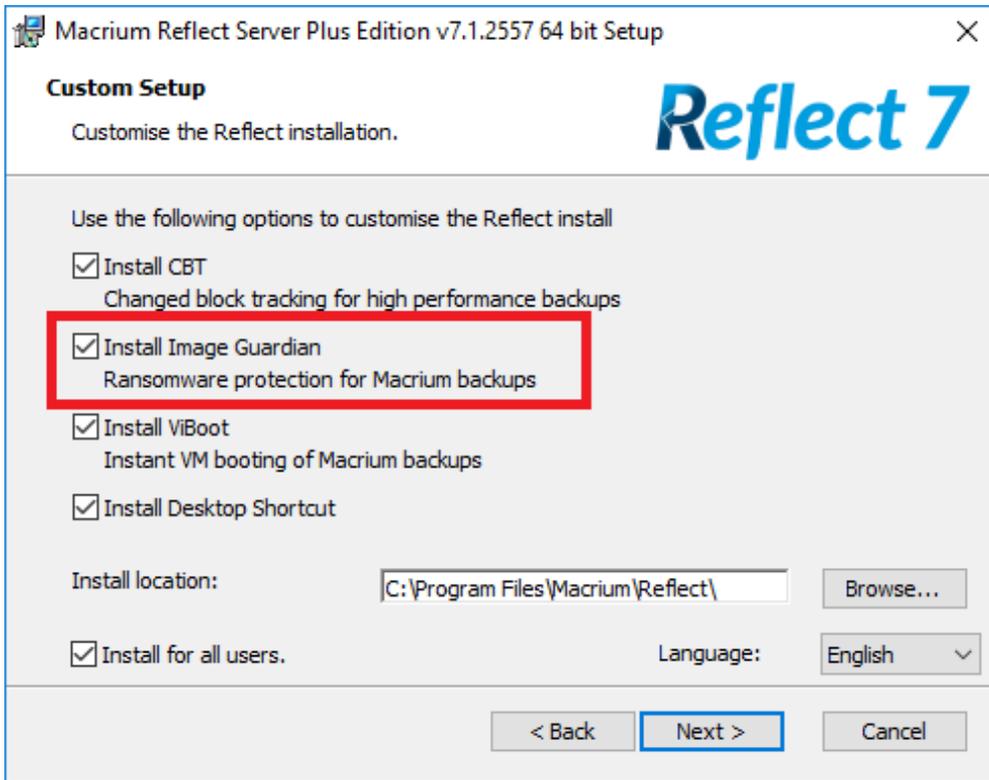
After installation, if **MIG has automatically protected any local back drives for existing backup definitions** then the following message box is displayed the first time Macrium Reflect is started:
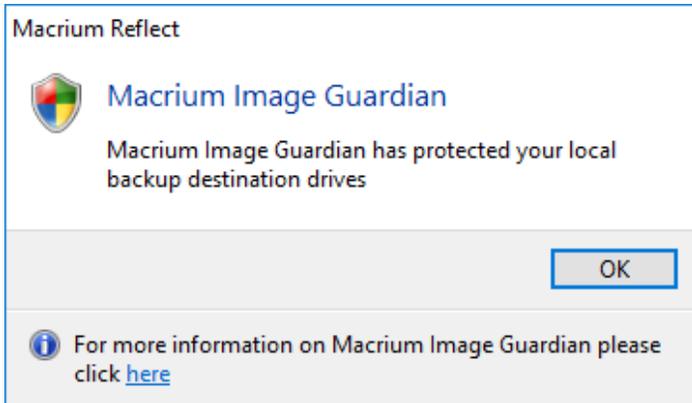
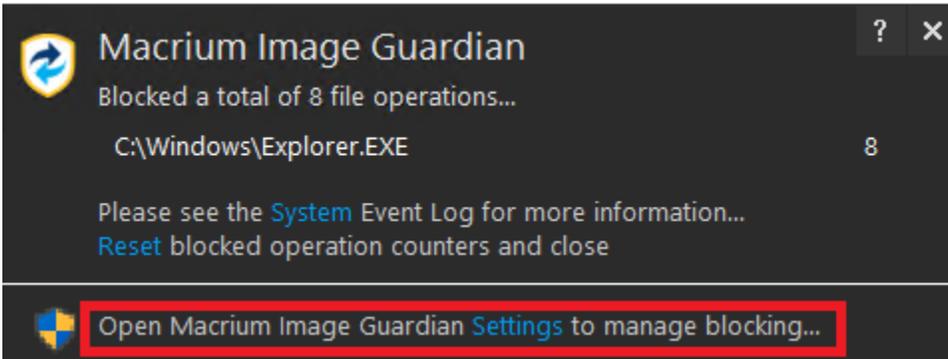## Activating Macrium Image Guardian

MIG is active directly after installation and will automatically protect backup destination drives.

To turn MIG on, off or temporarily disable **take the 'Other Tasks' > 'Macrium Image Guardian Settings..'** menu option.
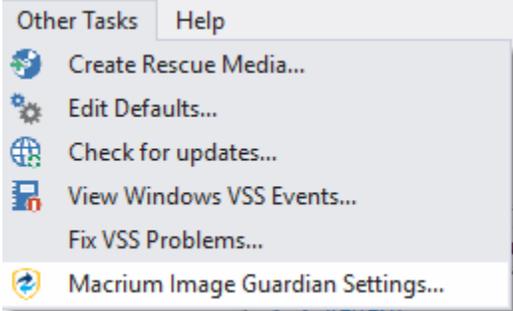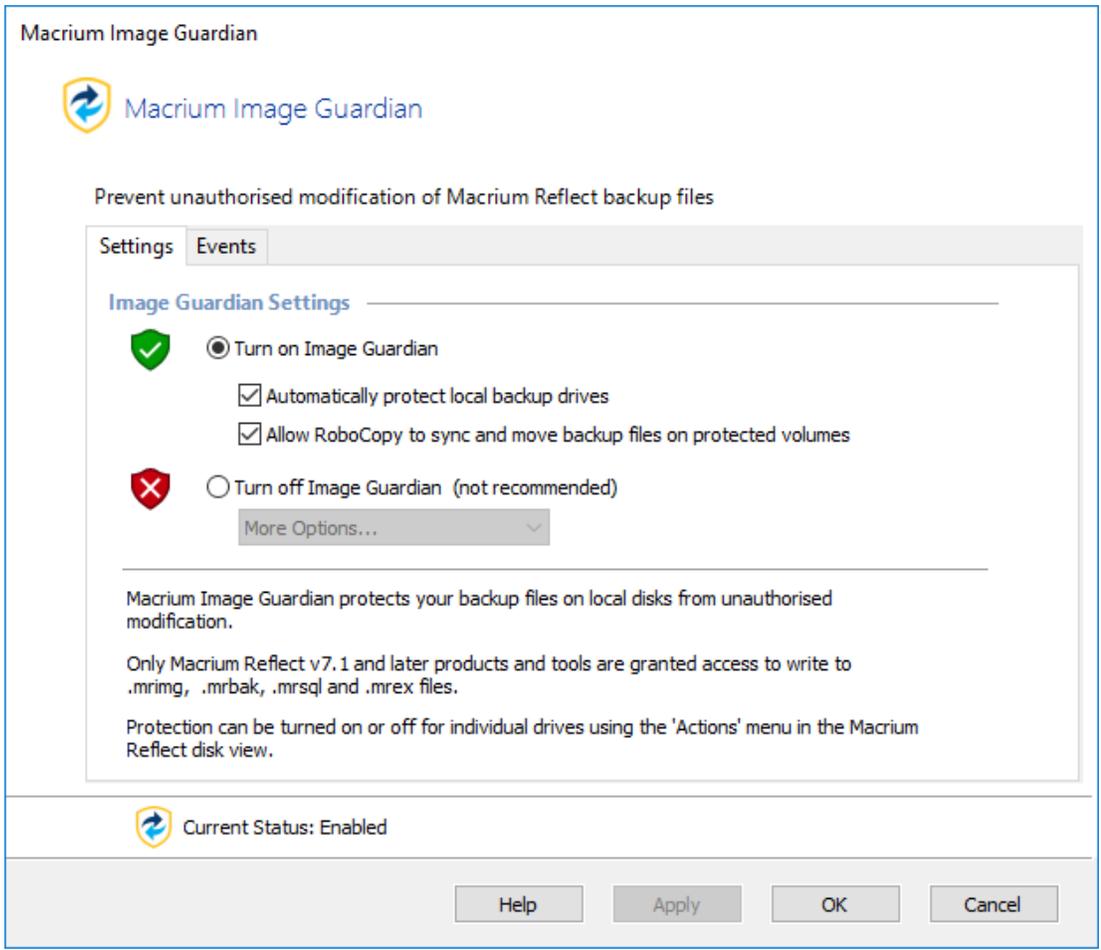

You can also activate the MIG Settings dialog by **clicking 'Settings'** in the MIG blocked activity popup.

The MIG Settings dialog

Turn on Image Guardian	Starts the Image Guardian Service
Automatically protect local backup drives	When turned on, all saved backup definitions are searched and Image Guardian is enabled for local backup drives When creating a new backups, unprotected target drives will be automatically protected by enabling Image Guardian on the drive. When the PC is restarted, Image Guardian will be re-enabled on all backup drives. This prevents accidentally leaving your drives unprotected by manually turning protection off.

Allow RoboCopy to sync and move backup files on protected volumes	Enables the MS utility RoboCopy to delete and overwrite backup files on protected volumes with the **/MOV, /MOVE, /PURGE** and **/MIR** parameters.

Parameter	Rule
/MOVE /MOV	If the **source folder** is on a protected volume then the **/MOVE /MOV** parameters will only delete backup files in the source folder if the **destination folder is also on a protected volume**. This ensures that existing files cannot be moved to an unprotected volume and compromised.
/MIR /PURGE	If the **target folder** is on a protected volume then the the **/MIR /PURGE** parameters will only delete backup files in the **target folder** if **both** of the following conditions are true: 1. The source folder **is** a backup destination in any saved backup definition xml file. 2. The target folder **is not** a backup destination in any saved backup defintion xml file This ensures that the synchronisation operation cannot inadvertently, or otherwise, delete files in a folder that is used as a backup destination in Macrium Reflect.
All overwrite operations	If the result of any parameter is to overwrite an existing backup file **on a protected volume** then this will only be allowed if the target folder **is not** a backup destination in any saved backup definition xml file.

RoboCopy and Network Shares

ⓘ

If the **source of a /MOVE /MOV** or **target of a /MIR /PURGE** operation is a **MIG protected volume on a network share** then all delete operations are **blocked.** This is because RoboCopy 'Rules' can only be applied if the Windows session that's opening the files is the same Windows session that's running RoboCopy. In the case of a network share, the remote computer is opening the files and will block all delete operations.

Turn off Image Guardian	Turns off the Image Guardian service. Optionally select from the list of further options:

1 Minute to 2 Hours	Select to temporarily disable MIG for the selected time
Restart service on reboot	MIG will remain 'Off' until the next Windows reboot.
Permanently Off	When 'Turn off Image Guardian' is selected, 'Permanently Off' is the defaulted option if MIG is currently enabled and nothing is selected in the 'More Options...' list. Otherwise, selecting this option will cancel any temporary disable settings and turn off MIG.

Note: Clicking 'Apply' will immediately change MIG and update the status text:.

The **status area** above the buttons shows the current status of MIG.


Current Status: Enabled

Current Status: Disabled

Current Status: Disabled Until Reboot

Current Status: Temporarily Disabled   MIG is disabled for: 04:28   Re-Enable

Clicking 'Re-Enable' will immediately cancel the outstanding temporary disable and **turn MIG 'On'.**

Macrium Image Guardian Events

To view Image Guardian windows events, **take the 'Other Tasks' > 'Macrium Image Guardian Settings..'** menu option and **select the 'Events' tab**:
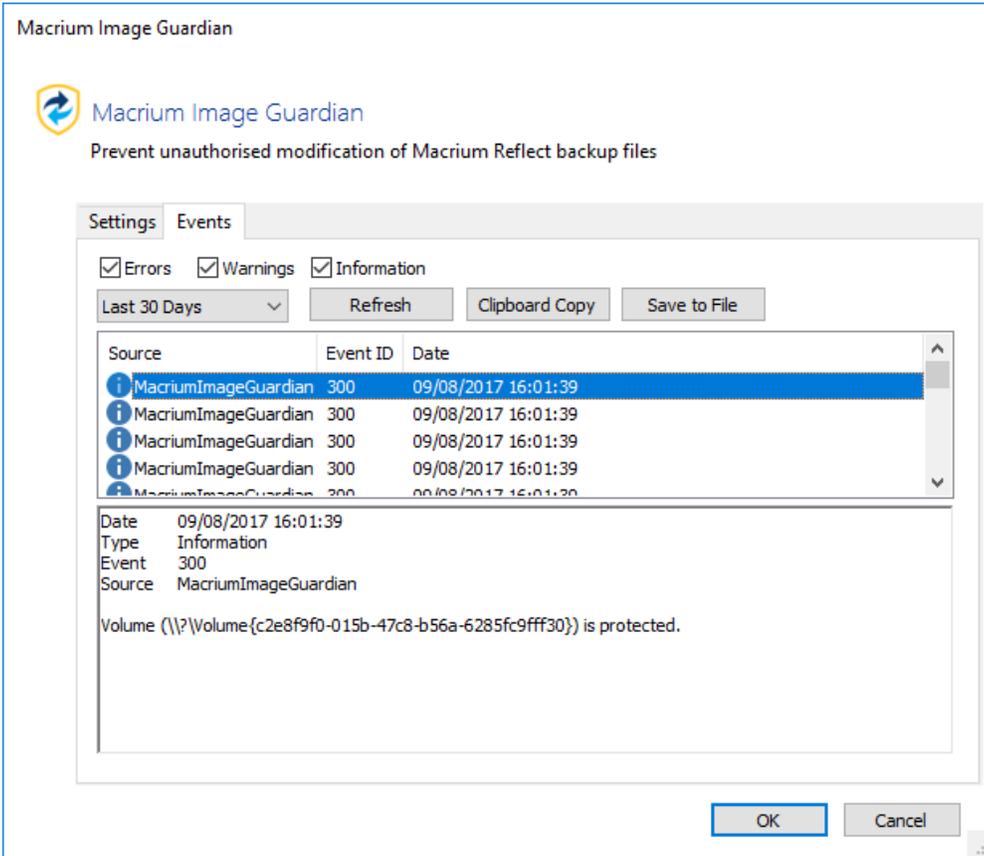

| Number	Event Name	Severity	Description
100	EVT_MIG_SERVICE_STARTED	Informational	Image Guardian service started
110	EVT_MIG_DRIVER_STARTED_BY_SERVICE	Informational	Image Guardian driver started by service
200	EVT_MIG_SERVICE_STOPPED	Informational	Image Guardian service stopped
300	EVT_MIG_VOLUME_PROTECTED	Informational	Volume (\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\) is protected
310	EVT_MIG_BLOCK_VERIFICATION_FILE_ACCESS	Informational	Blocking process (processname.exe) creating verification file as process is not Macrium certified
320	**EVT_MIG_BLOCKED_FILE_ACCESS**	**Warning**	**Blocked unauthorised process (processname.exe) accessing file (\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\Folder\filename.mrimg)**
330	EVT_MIG_USER_PROTECTED_VOLUME	Informational	User has enabled Image Guardian on volume (\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\)
340	EVT_MIG_USER_DISABLED_VOLUME	Informational	User has disabled Image Guardian on volume (\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\)
500	EVT_MIG_ERROR_BAD_EVENT	Error	Error could not open Image Guardian verification event. Error code = 123
510	EVT_MIG_ERROR_PROTECTING_VOLUME	Error	Error protecting volume (\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\). Error code = 123
520	EVT_MIG_ERROR_UNPROTECTING_VOLUME	Error	Error unprotecting volume (\\?\Volume{6a2d53fe-c79a-11e1-b189-806e6f6e6963}\). Error code = 123

When an unauthorised process attempts to write to, delete or rename a Macrium backup file the action will be blocked and Windows Event 320 will be generated

Enabling and Disabling MIG on NTFS Volumes

MIG can be enabled or disabled on any **NTFS volume** by using the **'Actions' menu** in the Macrium Reflect main window.
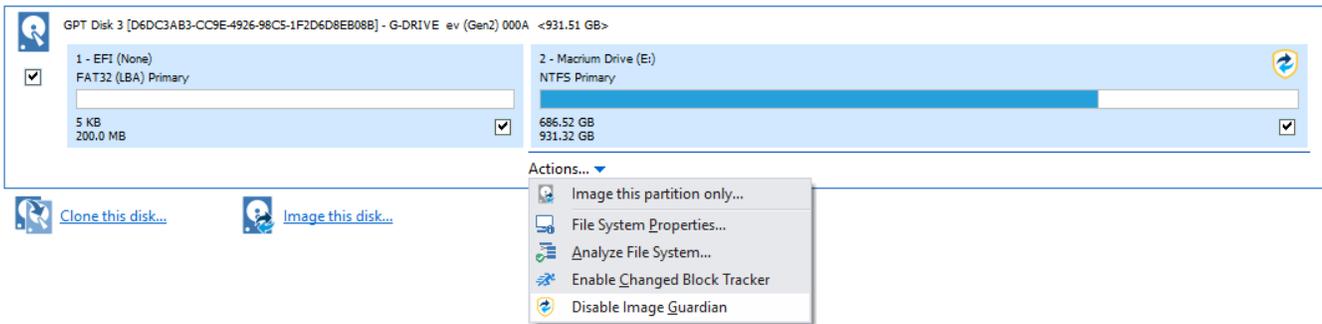
A **MIG** shield indicates that a volume is protected:
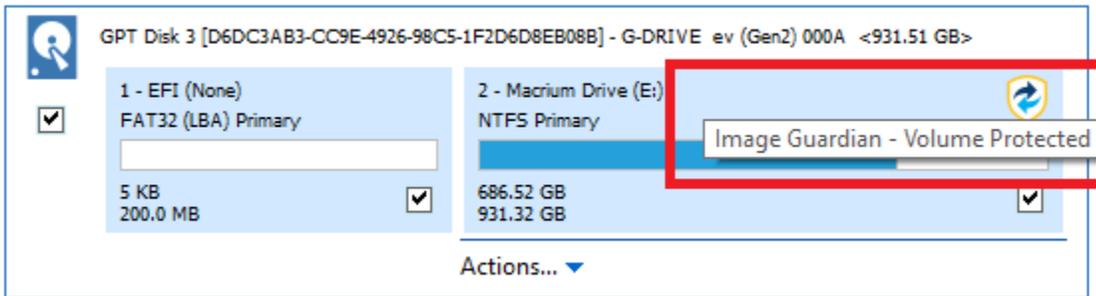
Automatic Protection

Please note that if the option to **'Automatically protect local backup drives'** is selected in the MIG settings dialog, then **unprotected volumes** will be **automatically protected** when the next backup runs to the volume, or on reboot, if the volume contains the path of a backup destination saved in a backup definition.