Adding BitLocker support to Windows PE

Note: It isn't absolutely necessary to unlock a BitLocker encrypted drive when restoring an image of the encrypted partition. The partition will restore without problems but will require re-encrypting on reboot.

Unlocking the drive in Windows PE enables intelligent sector copy imaging and cloning, RapidDelta Restore (RDR) and also free access to the drives contents using PE Explorer. In addition, restoring to an unlocked drive will retain the encryption status of the drive when rebooting.

Automatically unlocking BitLocker encrypted drives

Macrium Reflect can include the components and decryption keys necessary to automatically unlock Microsoft BitLocker encrypted drives in Windows PE.

In the Rescue Media Wizard select 'Include optional components' and 'Automatically unlock BitLocker encrypted drives'.

Rescue Media Wizard
Prepare Windows PE Image Select your architecture and WIM Type, then press next
Use the Windows Assessment and Deployment Kit to prepare the Reflect PE image
Build the PE Environment
PE Architecture: 64 Bit
 Include optional components - required for iSCSI and BitLocker support Automatically unlock BitLocker encrypted drives
Object to the set of the set o
Custom base WIM
For advanced users, a custom WIM enables you to prepare your own Windows PE environment.
Please press the Next button to continue.
Help < Back Next > Cancel Finish

When Windows PE starts any BitLocker locked drives that were attached when the recovery media was created it will automatically unlocked them.

Unlocking BitLocker encrypted drives using a USB stick

Automatically unlocking encrypted drives when PE starts may present an unacceptable security risk for some users. Automatic unlocking requires no user intervention and the Macrium Reflect boot menu is able to access encrypted drives without password entry. An alternative method is to **de-select** the **'Automatically unlock BitLocker encrypted drives'** option in the rescue media Wizard:

Rescue Media Wizard	
Prepare Windows PE In Select your architecture and WIM T	0
Use the Windows Assessment and [Deployment Kit to prepare the Reflect PE image
Build the PE Environment	
PE Architecture:	64 Bit 🔹
	nponents - required for iSCSI and BitLocker support nlock BitLocker encrypted drives
 Default base WIM (Recommended) Custom base WIM 	C:\ProgramData\Macrium\Reflect\Windows Kits\10\A\winpe.wim
For advanced users, a custom WI	IM enables you to prepare your own Windows PE environment.
	Please press the Next button to continue.
Help	Cancel Finish

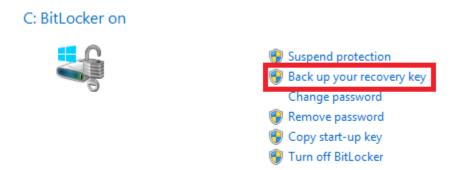
You can then save BitLocker Encryption Key files (.BEK) and/or BitLocker password TXT files to the root of any USB stick. This could also be a Windows PE rescue media USB stick.

1. In Windows Explorer, right click on any BitLocker encrypted drive and click on 'Manage BitLocker'.

Local Disk (C:) 39.4 GB free of 49.6 GB		Macrium Reflect Technician's USB	
59.4 GB Tree of 49.0 GB		Open Open in new window Change BitLocker password Manage BitLocker	
		Macrium Reflect Share with Pin to Start Format	
		Copy Create shortcut Rename Properties	

Macrium Reflect KB

2. In the newly opened window click 'Back up your recovery key'



3. In the BitLocker Drive Encryption wizard select 'Save to a USB flash drive' and chose the USB device you want to save to.

BitLocker Drive Encryption (C:)	
How do you want to back up your recovery key?	
Some settings are managed by your system administrator.	
A recovery key can be used to access your files and folders if you're having problems unlockin It's a good idea to have more than one and keep each in a safe place other than your PC.	g your PC.
Save to your Microsoft account	
 Save to a USB flash drive 	
 Save to a file 	
Print the recovery key	
What is a recovery key?	
	Cancel
	Cancel
Save a recovery key to a USB flash drive	
Insert the USB device, select it in the list,	
and click Save.	
Macrium Reflect Technician's USB (D:)	
Machum Reflect Fechnician's OSB (D.)	

After choosing the USB device you want to save the Recovery Key file to, **click 'Save'** and then '**Finish**' in the BitLocker Drive encryption wizard. This action will save a .BEK file and/or a recovery password text file to the chosen USB device.

Note: The .BEK file is a protected operating system file, it is hidden by default and won't be visible within Windows Explorer. it can be made visible by changing Folder Options and de-selecting the option to '**Hide Protected operating system files**'.

You can add as many keys as you have encrypted drives.

When Windows PE starts ensure that your USB flash drive is attached to your PC. Your encrypted drives will then be automatically unlocked when Macrium Reflect initializes.