

DESlock+ Full Disk Encryption Known UEFI Boot Issues

DESlock+ Technical Bulletin January 2015

Version	1.3
Date	27 th January 2015
Status	See change history



Table of Contents

Purpose	3
Change History	3
Useful References.....	3
Symptom	4
Cause	5
Identifying the problem.....	5
Booting the System	6
Resolving the issue	7
Systems known to exhibit the problem.....	7
Accessing the Boot Menu – Additional Information	8
Key Combinations.....	8
Enabling the Boot Menu.....	8



Purpose

Since the release of DESlock+ with support for UEFI and GPT Disks it has been discovered that the UEFI firmware implementation on some systems does not follow the UEFI specification correctly.

This information applies to the DESlock+ Client version 4.7.4 and version 4.7.5.

Note: the issues described in this document affect systems configured in UEFI mode with GPT disks and does not apply to traditional BIOS mode with MBR disks.

Change History

VERSION	DATE	AUTHOR	DESCRIPTION
1.3	27 th January 2015	Duncan Hume	Added Toshiba Satellite C55 & C50 to known systems.
1.2	14 th January 2015	Duncan Hume	Added data loss warning for Windows 8 system repair section. Updated boot key combination details to make clearer.
1.1	14 th January 2015	Duncan Hume	Added more information about accessing the boot menu. Added Acer Aspire S7 to known systems.
1.0	13 th January 2015	Duncan Hume	Initial draft

Useful References

Article ID: KB103 - How can I tell if my computer is using UEFI?

<http://support.deslock.com/KB103>

Article ID: KB193 - Windows 8 can enter Automatic Repair following DESlock+ Full Disk Encryption

<http://support.deslock.com/KB193>



Symptom

Once the system is Full Disk Encrypted and has rebooted for the first time, it will not boot and the operating system displays an error.

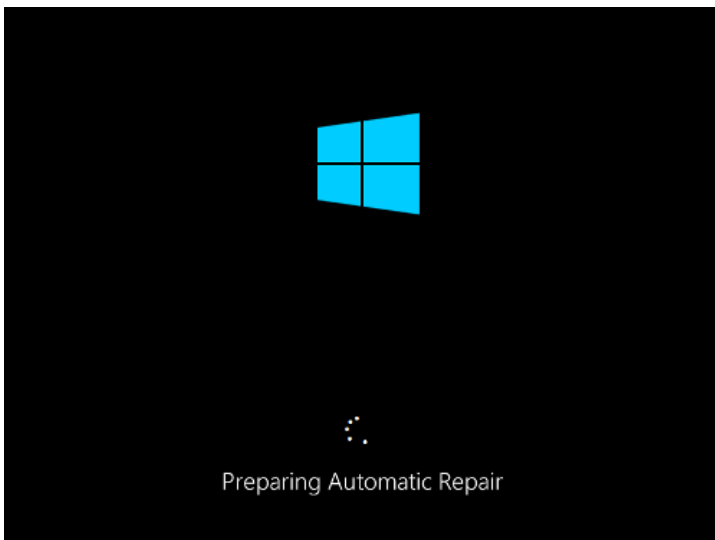
The error shown depends on the operating system and the UEFI implementation.

Windows 7



Windows 7 fails to boot with a status of 0xc000000f : “The boot selection failed because a required device is inaccessible” .

Windows 8 and 8.1



Windows 8 enters Automatic Repair on start-up, continuing with Automatic Repair is unable to resolve the problem.

It is important to let the Automatic Repair complete, even though it will be unable to resolve the problem. Restarting or turning off the system while the repair is in progress can result in irrecoverable data loss.



Cause

The problem is caused by poorly implemented UEFI firmware. Generally the firmware ignores the programmed boot order and attempts to directly boot the Windows UEFI boot loader. This causes the DESlock+ boot loader to be bypassed, this skips the code necessary for the system to be decrypted, resulting in an unbootable system.

Several variations of the flaw have been seen with different firmware implementations:

1. The firmware simply ignores the UEFI boot order in NVRAM and boots directly to the Windows boot loader.
2. The firmware re-writes the boot order, placing the Windows boot loader at the head of the list.
3. The firmware clears the boot list written to NVRAM, leaving only the Windows entry.

Identifying the problem

Currently the only way to identify the problem is to attempt Full Disk Encryption. Safe Start* mode should be used, however this will not always be able to protect against the problem due to how the UEFI firmware is implemented on some systems.

When Full Disk Encryption is started in Safe Start mode, some systems will bypass the Safe Start test after the reboot. In these cases Full Disk Encryption will not continue.

On some systems Safe Start is known to succeed, but the UEFI firmware will still bypass the DESlock boot loader. In these cases Full Disk Encryption will begin as normal, however upon reboot the system will not start as described in [Symptom](#)

**Safe Start provides a means to test for Full Disk Encryption compatibility, by installing a special boot loader and rebooting the system. If the system boots correctly through the Safe Start boot loader then Full Disk Encryption commences. If the system does not boot correctly, or the Safe Start boot loader is bypassed, then the system is restored to normal and no encryption takes place. Safe Start is optional when DESlock is managed by an Enterprise Server and mandatory when unmanaged (standalone).*

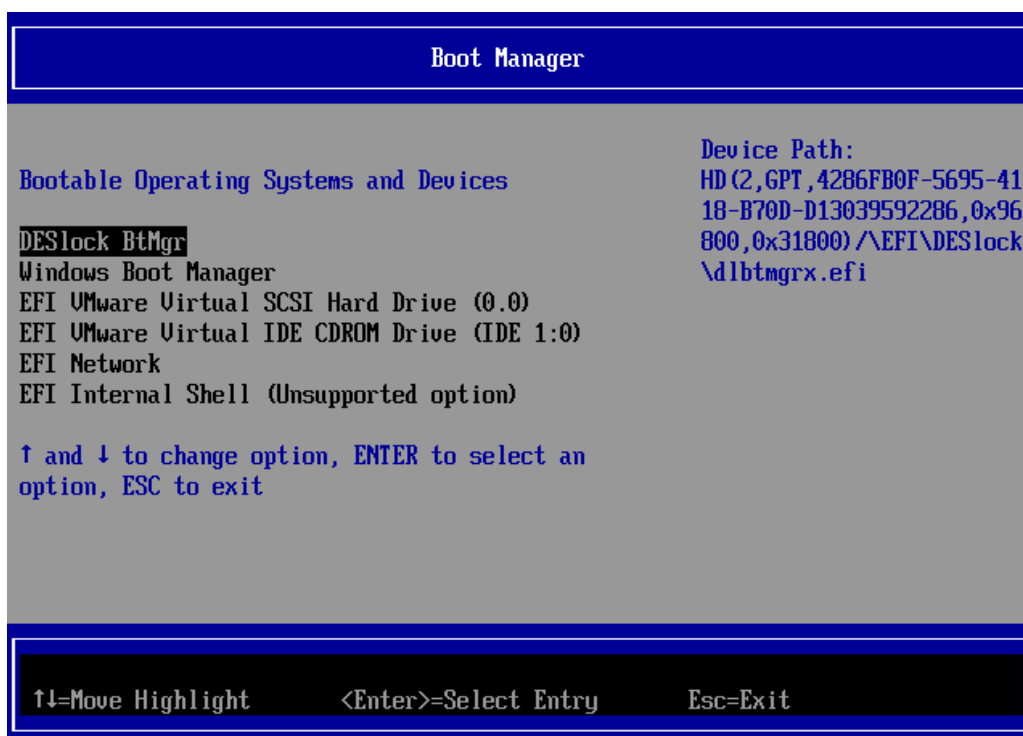


Booting the System

To correctly boot the system you will need to enter the "UEFI Boot Menu" and choose the DESlock+ boot menu option.

Boot the PC. As the firmware starts to run, press the key that opens the boot device menu. For example, press the Esc, F2, F9, F12, or other key to enter the firmware or boot menus. You will need to refer to your hardware documentation for details on entering the EFI boot menu. The manual may alternatively refer to it as "Boot Option Menu" or some other term. Please see [Accessing the Boot Menu – Additional Information](#) section for further information.

Once you have found the boot menu, it will display a list of options, similar to the below.



You must choose the **DESlock BtMgr** option to boot to the DESlock+ login. You can then enter credentials to boot the PC normally.



Resolving the issue

Until you are able to resolve the issue correctly you may need to go through the process of manually selecting the boot item each time you wish to boot your PC. It is possible this may be fixed in a firmware update to the hardware.

Although this is known to be a flaw in the system manufacturers UEFI implementation, the DESlock development team is working hard to produce a workaround and allow DESlock+ to function correctly despite of these flaws. The next release of DESlock+ is expected to include this workaround.

Please see our support news page and subscribe for updates to be notified of when a new version is available.

<http://support.deslock.com>

Please note: If you plan to update the system UEFI firmware it is recommended that you decrypt the system first. Updating the UEFI firmware can clear the system NVRAM and remove the DESlock boot entry entirely.

Systems known to exhibit the problem

To date, HP systems using UEFI firmware provided by Chinese manufacturer Insyde have been the most reported, however the problem is not isolated to HP or Insyde.

Manufacturer	Model	Bios	Type
Acer	TravelMate TMP-256-M-55EG	Insyde V1.13	Laptop
Acer	Aspire S7-391 (MS2364)	Insyde V2.18	Laptop
Dell	Vostro 3360	DELL / Phoenix	Laptop
HP	Pavilion G6	Insyde F.29	Laptop
HP	Pavilion TS 23-F200EJ	AMI 80.08	All in One Desktop
HP	Envy TS Sleekbook 4	Insyde F.23	Laptop
HP	Envy 4-1202EA	Insyde F.21	Laptop
Sony	VAIO svt1312v1es	Unknown	Laptop
Lenovo	ThinkPad S1 Yoga 20CD00B1CA	LENOVO 1.09	Laptop / Tablet
Toshiba	Satellite C55-B866	Unknown	Laptop
Toshiba	Satellite Pro C50-A-1E2	Unknown	Laptop

If you have details of other systems that exhibit this problem, or would like to beta test the new release when available, please contact DESlock support by creating a support ticket:

<http://support.deslock.com/index.php?/Tickets/Submit>





Accessing the Boot Menu – Additional Information

For the most complete information on accessing the systems BIOS and UEFI boot menu, please see the hardware documentation that came with your system. Alternatively the information should be available from the manufacturer’s website.

Key Combinations

Some laptops do not have dedicated function (F) keys and you must press a key combination.

For example for **F12** you might have to press   simultaneously.



Enabling the Boot Menu

Some systems can also have the boot menu disabled with in the BIOS. If you are unable to access the boot menu using the correct key press, check the BIOS menus to see if the boot menu is disabled.

For example: *Enabling the F12 function on an Acer system:*

1. Power on the system. As soon as the first logo screen appears, immediately press the F2 key, or the DEL key if you have a desktop, to enter the BIOS.
2. Press the right arrow key to select Main.
3. Use the arrow keys to navigate to F12 Boot Menu, and press ENTER.
4. Select Enabled, and press ENTER.
5. Press the F10 key to save changes and restart the system.

