

TECH CENTER



Portaal > Kennisbank > ESET Endpoint Encryption > How do I decrypt a standalone system that is unable to start Windows?

How do I decrypt a standalone system that is unable to start Windows?

Anish | ESET Nederland - 2018-03-07 - 0 Comments - in ESET Endpoint Encryption

Should your full disk encrypted machine suffer a Windows error that prevents Windows from starting correctly, you may be required to decrypt the disk in order that Boot CD and other Windows recovery methods are able to access the disk contents to correct the error.

To do this you can use the Full Disk Encryption recovery ISO image to burn a CD to boot and decrypt the system without requiring Windows itself to load.

The recovery image can be downloaded

here: <http://download.deslock.com/download/utility/recovery.iso>

Please note if your system is managed by an Enterprise Server then please see this alternative guide: [KB210: How do I decrypt a managed system that is unable to start Windows?](#)

If the CD does not boot at all, please check if your PC uses **UEFI** in the BIOS. The recovery CD requires the BIOS in **Legacy** mode and may require you to change the setting. You will need to remember to set it back afterwards.

Some PCs offer a boot menu that allows you to boot from a CD after pressing a key, if this is not available, you may need to change the boot order in the BIOS to put the CD/DVD drive first.

Decrypting the Workstation

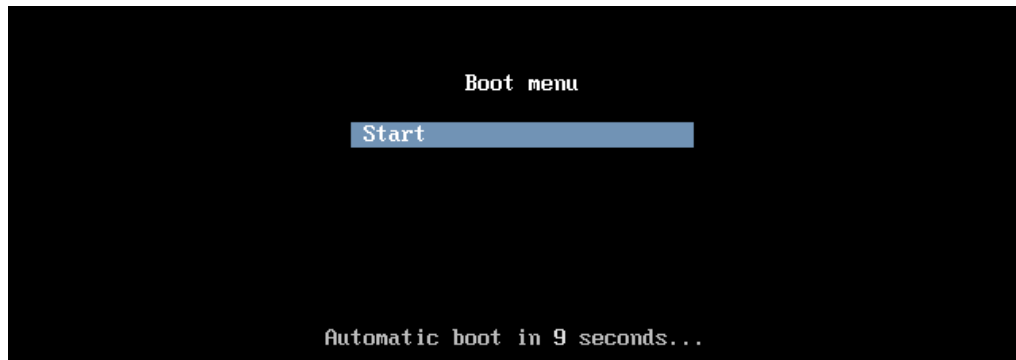
It is recommended that where possible a sector level backup of the machine is taken before starting the recovery process.

If the machine being recovered is a laptop you should ensure it is connected to its power supply before starting the decryption process.

Decryption of the disk will take longer than it took to encrypt it originally and **must** only be interrupted by pressing **Esc**.

Burn the generated CD image to a blank CD and use this to boot the Workstation.

You should be greeted by a splash screen, press **return** or wait a short while for the software to launch.



The recovery app will launch, press the **Return** key to continue.

```
o1/input/input5
[ 4.163229] parport_pc 00:08: reported by Plug and Play ACPI
[ 4.163294] parport0: PC-style at 0x378, irq 7 [PCSP,TRISTATE]
[ 4.175957] Error: Driver 'pcspkr' is already registered, aborting...
[ 4.195769] ENS1371 0000:02:02.0: PCI INT A -> GSI 16 (level, low) -> IRQ 16
done.
Activating swap...done.
Loading kernel modules...done.
Fast boot enabled, so skipping file system check. ... (warning).
Mounting local filesystems...done.
Activating swapfile swap...done.
Cleaning up temporary files....
Cleaning up temporary files....
INIT: Entering runlevel: 2
Using makefile-style concurrent boot in runlevel 2.
[ 5.241576] end_request: I/O error, dev fd0, sector 0
[ 5.261546] end_request: I/O error, dev fd0, sector 0

DESlock+ Full Disk Encryption Recovery Tool - Version 1.2.1 (Build 15)
Copyright (c) 2013 DESlock Limited

Press Return to continue
```

If the Recovery tool is unable to locate the DESlock+ encryption information, it will offer to search for the required boot files. Please see <http://support.deslock.com/KB222> for more details.

Type the word **DECRYPT** then press **Enter**.

```

Detecting devices...

Encrypted drives or partitions found

*****
**                               !WARNING!                               **
*****
**                               **                                       **
** IT IS VITAL THAT YOU LET THE DECRYPTION PROCESS FULLY **
** COMPLETE, OR STOP IT CORRECTLY BY PRESSING ESC.      **
** REBOOTING OR REMOVING POWER WHILST DECRYPTION IS IN  **
** PROGRESS MAY LEAD TO IRRECOVERABLE DATA LOSS!       **
**                               **                                       **
*****

Please Note : Keyboard input is US English ONLY

Please type DECRYPT and press Return to continue, anything else will abort.

```

Type the admin password then press **Enter**. This password was recorded when you initially encrypted the machine and would have been saved to a file called adminpassword.txt or adminpassword.htm. See this article for more detail: ['Why do I need an admin password?'](#)

The latest versions of the Recovery CD allow any user to start decryption, provided it is in Standalone mode, as shown below

```

Detected Usernames:
Names : 'admin', 'user1', 'user2'
Please enter a username: _

```

However, on a Managed system, you can only use the 'admin' user, as shown below. Note: The actual username may be different as it can be specified in the Enterprise Server.

```

This is a Managed workstation, only the FDE Admin user can be used.
If you do not have this, you should use the FDE Recovery Image from your Enterprise Server.

Please enter the password for the user 'admin' to begin decryption
NOTE: Password characters WILL be displayed on screen
Enter password: _

```

Note: If you have used Auto FDE ([KB441](#)), a user and password is not required, decryption will start immediately.

Providing the correct password is supplied, decryption will start. Note: It is very important you let the process complete and **DO NOT** shutdown or power the machine off, you must press Esc and wait to be prompted.

```

** REBOOTING OR REMOVING POWER WHILST DECRYPTION IS IN **
** PROGRESS MAY LEAD TO IRRECOVERABLE DATA LOSS! **
**
*****

Please Note : Keyboard input is US English ONLY

Please type DECRYPT and press Return to continue, anything else will abort.
decrypt
Detected Usernames:
Name: 'admin'
Name: 'kbtest'

Please enter the password for the user 'admin' to begin decryption
NOTE: Password characters WILL be displayed on screen
Enter password: theadminpassword

Encrypted items: 1
Decrypt disk 0:0
Decryption in progress, do not shutdown or power off, press ESC to stop.
Decrypting : please wait
Decrypting : sector 169984 of 6346752 (est. time 0h02m26s)

```

Once decryption is complete press **Enter** to restart the machine.

```

Name: 'kbtest'

Please enter the password for the user 'admin' to begin decryption
NOTE: Password characters WILL be displayed on screen
Enter password: theadminpassword

Encrypted items: 1
Decrypt disk 0:0
Decryption in progress, do not shutdown or power off, press ESC to stop.
Decrypting : please wait
Decrypting : device complete

Zero cached status block
Zero status block @ 5721284

Decryption of disk complete
Everything decrypted. Restore system mbr
Restoring master MBR on disk 0:0...

Your system has been successfully decrypted

Please press the Return key to restart the system

```

Remove the CD from the systems CD tray, when the system restarts it should boot straight to Windows without showing the DESlock+ pre-boot login screen.

Keywords: recover, windows, error, fail, boot, decrypt, iso, standalone