ESET Tech Center

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

Anish | ESET Nederland - 2018-03-07 - Reacties (0) - 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.

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**.

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

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.

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.

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

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