ESET Tech Center

DESlock+ Full Disk Encryption Recovery Overview

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

The following article describes the various scenarios involved in Recoverying a DESlock+ Full Disk Encrypted system that either no longer boots or has suffered some form of corruption on the disk.

Please note, you should not try to perform any repairs yourself using 3rd party tools and Windows automatic repair should be allowed to complete rather than cancelled as these could lead to irrecoverable data loss.

If the machine you are attempting to decrypt will not boot due to a hardware failure, then you can connect the encrypted disk to another machine as the **only** connected disk. The disk **must** be connected as a bootable device. Once connected correctly, follow the relevant article from the list below.

Please note: connecting an encrypted disk via a caddy, or similar connection, will **not** work.

Standalone FDE

Where a system can boot a CD or USB stick, via BIOS or Legacy boot mode, follow KB211 - How do I decrypt a standalone system that is unable to start Windows?
Where the standard recovery ISO fails to boot or where the system only has UEFI boot mode, follow KB281 - How do I decrypt a system that only has UEFI boot mode?

Managed FDE

Where a system can boot a CD or USB stick, via BIOS or Legacy boot mode, follow KB210 - How do I decrypt a managed system that is unable to start Windows?
Where the standard recovery ISO fails to boot or where the system only has

UEFI boot mode, follow KB281 - How do I decrypt a system that only has UEFI boot mode?
Where the system is Full Disk Encrypted using a TPM, follow KB448 - Recovery on TPM systems with only UEFI boot mode.

Other Scenarios

Where a system has been sent a Disable command from the Enterprise Server, follow KB210 - How do I decrypt a managed system that is unable to start Windows?
If the Admin user has not been wiped, and KB210 does not work, you can try following KB281.
Where a system had FDE started from an Enterprise Server, but is now being used Standalone, follow the KBs in the Standalone FDE section, however you MUST know the Admin users password.
Where the Recovery Tool won't allow decryption because it reports **Master Disk is missing required data**, please create a support ticket that includes as much detail as possible. If the system is Managed, please include a Workstation Log (KB320). It may still be possible to recover the system, but it may require access to the disk in another system.
Where the DESlock+ Pre-Boot Authentication is not shown, the MBR may have become damaged or replaced, follow KB222 - Repairing the DESlock+ Full Disk Encryption MBR using the recovery tool.
Where FDE was started automatically (KB441 - Automatically Starting Full Disk Encryption (FDE)), and no Pro licence users have been activated, follow KB211 - How do I decrypt a standalone system that is unable to start Windows? **or** KB281 - How do I decrypt a system that only has UEFI boot mode?