ESET Tech Center

Windows 10 Compatibility

Anish | ESET Nederland - 2018-02-07 - Comments (0) - ESET Endpoint Encryption

Windows 10 is supported with DESlock+ client v4.8.0 and later, and DESlock+ Enterprise Server v2.6.0 and later.

Prerequisites

For Windows 10 machines running build version 10240 must have the cumulative updates installed. For more information read this article: KB273 - Cumulative Update for Windows 10 must be installed before DESlock+ (This applies to the DESlock+ client only)

Upgrades/Updates

Full Disk Encryption

If you are upgrading or updating from Windows 7, 8, 8.1 or an earlier version of Windows 10 to the latest version of Windows 10, and have Full Disk Encrypted your machine, the upgrade will fail. To avoid this, follow this article here: KB379 - Installing Windows 10 Feature Updates on an Full Disk Encrypted (FDE) system

Folder Encryption

If you are using DESlock+ encrypted folders with your existing operating system it is recommended you **first uninstall** DESlock+ before upgrading to Windows 10 as detailed here: KB97 - Uninstalling DESlock+

Once the upgrade of the operating system is complete the DESlock+ client can be reinstalled.

Failure to remove DESlock+ before updating may mean your encrypted folders will be not located in their normal location. Instead an empty folder will be located there instead. The original encrypted folder, containing your encrypted data, will instead be found in the folder **Windows.old** on the root of the system disk.

e.g. the folder *C:\Users\"user"\Desktop\encrypted folder* will be found

in *C:\Windows.old\Users\"user"\Desktop\encrypted folder*

Known Issues

(Resolved in version 4.8.0 onwards)

When using the previous release version of DESlock+ v4.7.8 on test systems with Windows 10, we observed the following issues:

Systems became unresponsive to keyboard input and would not redraw the screen correctly at the Windows login screen or when resuming from hibernate/standby. The problem was more likely to occur the longer the operating system is left at the login screen.
Some systems were not be able to shutdown correctly once full disk encryption has been performed and the system would remain powered on requiring a forced power cycle to clear.