ESET Tech Center

Windows User context and encryption

Anish | ESET Nederland - 2018-02-16 - Comments (0) - ESET Endpoint Encryption

The context of the user can have an affect on how and what encrypted storage they are able to access as detailed below.

Sessions

When a user enters their DESlock+ Key-File password it allows their user session within Windows access to encrypted containers that were encrypted using encryption keys they have available. i.e. Virtual Disks and Encrypted Removable Media become available for access.

If another user logs in to Windows at the same time as the original user, then even with the appropriate key they will have some limited access to those same containers. In the case of removable media they will be denied access to the encrypted storage and in the case of virtual disks they will be given read-only access.

Users

Some software, while launched from the within the users session may elevate itself when running or run under the *System* user account. If this happens then encryption keys will not be available to that software's process and access will be denied to the containers.

Some example scenarios where the above behaviour may be experienced are:

- Another user is attempting to access the encrypted data across the network.
- The user has elevated software by using the 'Run as administrator' option and is being denied access to the encrypted containers from the software.
- Software is running under a different user context within the users session. e.g. backup software which runs under the System user account possibly as a Windows Service.

The above behaviour does not apply to Full Disk Encryption of system disks. However if you intend to use backup software with an encrypted system disk you should ensure that restoration has been tested using the solution in question before deploying to a live environment.

In most instances a file style sync backup of data from full disk encrypted systems would be the best route to use for scheduled backups. Backups performed at a file level are more likely to run as the user instead of the system so also have the benefit they have access to encrypted storage should it be required.

It is possible to mount a virtual disk globally so all users on the system will be able to access its contents. This is done using the command line tool detailed here: KB186 - Using the DESlock+ Command Line Tool

Related article: KB198 - I am unable to encrypt a network folder

Keywords: access, denied, 0x80070005