

Standalone Client Encryption Keys

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

This article is for users using the software in a standalone capacity without an Enterprise Server.

Encryption Keys

Encryption of granular data (i.e. Encrypted Files, Encrypted Folders, Encrypted Removable Media, Encrypted Emails, Encrypted Archives, Encrypted Virtual Disks) is performed using **Encryption Keys**. These encryption keys are stored in a file on the system known as the **Key-File**.

Access to the Key-File is provided by the user entering their password in the DESlock+ login dialog.



Obtaining Encryption Keys

Encryption keys can be added to the Key-File in three different ways:

1. When performing the initial setup the licence wizard allows a default encryption key to be created as part of the setup process.



2. From within the Key Manager using the Generate button.



3. By transferring a copy of an encryption key from another user as detailed here : [How do I share an encryption key with another DESlock+ user?](#). If a key has been obtained in this way then it will keep the same serial number of the originating copy.

When encryption keys are generated they are unique and created on your computer. No encryption key or password information is sent to deslock.com.

Therefore it is very important that backups of the key-file are taken in case the operating system drive containing the Key-File suffers a failure and you remember the password to the Key-File. Please see this article for details: [How do I backup my Key-File?](#)

Serial Numbers

Each user has a unique Key-File serial number which is tied to their DESlock+ licence. When an encryption key is generated it is given a serial number that contains the Key-File serial number with an index number at the end of it. This index increases each time an encryption key is generated on the system.

You can view the serial number of an encryption key by selecting it in Key Manager.



Note: If you were to restore a Key-File backup onto a second system and then generate a new encryption key on both machines, both systems would list the new key as having the same serial number in the Key Manager. However the encryption key data itself would be different and they would be **unable to decrypt** data that was encrypted with the other.

Keywords: restore, new, pc, license