ESET Tech Center

What is a Key-File and why is it important?

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

In common with other encryption products, DESlock+ can use a shared password to share encrypted files, archives, email Etc. However, these passwords cannot be backed-up by an Administrator, are often forgotten and frequently written down. Encrypting shared information with a Key is a far more manageable process, less likely to be compromised and much less likely to result in a user being locked-out.

Other systems do this through the use of Public Key Cryptography or a version of this and while highly effective and easy for competent technical users to work with, they may pose usability problems for nontechnical users. DESlock+ approaches this problem from a different angle and allows users to have up to 64 different encryption keys at the same time. These encryption keys may be shared with separate and overlapping user groups and by doing the exact equivalent of what we all do with physical keys in our everyday lives DESlock+ provides a wholly intuitive means of allowing users to share encrypted information securely.

A Key-File is an encryption key container that can hold up to 64 unique encryption keys. These encryption keys make the encryption of your computer, USB memory stick/hard drive, emails and files possible.

The Key-File is important because it is unique to your computer/organisation, it acts as an identifier to allow communication between devices and parties providing they share the same encryption key therefore making them recognisable. It is important to ensure that the Key-File is backed up as it is specific to all of your encrypted machines and devices.

In a managed environment the DESlock+ Enterprise Server manages the distribution of encryption keys among users ensuring that if necessary the encryption key required to access data is never lost.

For unmanaged users DESlock+ prompts to backup when new encryption keys are created or added to a Key-File. Unmanaged users can also share encryption keys with other unmanaged users via the Key Transfer Wizard. If you inadvertently forget your DESlock+ password and don't have access to another Key-File to containing the encryption key, or a previous backup with a

different password set there is no way to access your data.

Related articles

KB58 - How do I backup my Key-File?