ESET Tech Center

Which algorithm is used for encryption?

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

Full Disk Encryption

When Full Disk Encrypting a computer's hard drive, it uses the Advanced Encryption Standard (AES) algorithm with a 256 bit key. This encryption key is generated at the point of full disk encryption being started.

Removable Media Encryption

All encrypted data on Removable Media uses Advanced Encryption Standard (AES) algorithm with a 256 bit key and is applicable whether using Full Disk Encryption or File & Folder Removable Media Encryption.

When encrypting Removable Media the user is prompted to choose an encryption key from their Key-File which could be using either the AES, 3DES or Blowfish algorithms.

The chosen encryption key is used to derive the AES256 key used for encryption and is not used for the encryption of data itself. This is preferred to using a password or pass-phrase to derive the key as it is more secure, and enables DESlock+ to provide seamless access to data on encrypted Removable Media when the end-user is logged into the DESlock+ Key-File.

Other encryption methods

For all other encryption containers the user can choose between AES, 3DES or Blowfish algorithms. When encrypting data the key type being used selects the algorithm.

Both AES and Blowfish keys have a length of 128 bits whereas 3DES has a key length of 112 bits.

You can view which encryption keys you have at your disposal by right clicking on the DESlock+ icon in the Notification Area (formally known as the System Tray) and clicking on 'Key Manager'. This will open the following Window which will display and if you are a stand-alone user allow creation of new encryption

keys.

Password Encryption

Password encryption uses a 192 bit AES key, not to be confused with Removable Media Encryption above.

Managed Users

If you are a managed user, you can only view encryption keys which have been made available to you by your Enterprise Server admin. Keys can be created and allocated to you by your administrator through the Enterprise Server.