ESET Tech Center

Using the DESlock+ Command Line Tool

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

The DESlock+ Command Line Tool allows access to specific DESlock+ functions through a command line interface. This can be useful if you need to automate actions within the DESlock+ client software.

There are two version of the tool available appropriate to the platform being used which can be downloaded here:

Download 64bit Command Line Tool

Download 32bit Command Line Tool

Note: This software requires DESlock+ v4.3.45 or later installed to function.

Login Operations

It is possible to login or logout of the user's key-file from the command line.

Login

To login to the Key-File use the *login* command and supply the *-p* switch followed by the Key-File password as shown below.

Example usage:

```
DLPCmd64 login -p:Password
```

Logout

To logout of the Key-File use the *-p* switch with no password as shown in the example below.

Example usage:

```
DLPCmd64 login -p:
```

Encrypted File and Text Operations

The DESlock+ Command Line Tool can be used to encrypt and decrypt files from a command prompt, using a DESlock+ encryption key or a password.

> ***The current user must have a setup Key-File and be logged in to DESlock+. These operations will not work from an elevated command prompt, as the users key-file cannot be accessed from the elevated task.***

There are 2 encryption methods supported:

Text mode encryption

This mode is compatible with DESlock+ Email and Text encryption.

Simply provide a text file to the tool and it will create an encrypted copy of the contained text so that it can be included in an email or document. This text can then be decrypted by the tool or by using DESlock+ Email or Text Encryption. You will need to specify a destination filename when using this method.

Example usage:

```
DLPCmd64 encrypt text keyname:"My Key" input.txt output.txt
```

File mode encryption

This mode is compatible with DESlock+ File Encryption (.dlp files)

Simply provide any type of file and it will be encrypted, creating a new file with a .dlp extension. This file can then be decrypted by the tool or by using DESlock+ File Encryption.

Example usage:

```
DLPCmd64 encrypt file key:80004D8300AF figures.xls
```

File mode decryption

Using the decrypt switch allows encrypted files to be decrypted.

You will need to pass the type of decryption to perform (file or text) and the source filename. If you are decrypting a text mode file then an output filename is also required.

Example usage:

```
DLPCmd64 decrypt file figures.xls.dlp
```

```
DLPCmd64 decrypt text safe.txt passwords.txt
```

Encrypted Folder Operations

The Command Line Tool can be used to create an encrypted folder or display the encryption status of a folder.

Create Encrypted Folder

To create an encrypted folder, pass the path of the required new folder name and either the encryption key name or encryption key serial number. If you wish to hide the folder from view when the user is not logged in then pass the *-h* switch.

Important: The destination folder must **not** already exist or the command will be rejected.

Example usage:

```
DLPCmd64 folder "C:\Secure Docs" keyname:3des
```

```
DLPCmd64 folder "C:\Secure Docs" key:8006BFB0001
```

```
DLPCmd64 folder "C:\Secure Docs" key:8006BFB0001 -h
```

Display Encrypted Folder Status

The encryption status of a folder and how it is encrypted can be shown by passing the folder path without any encryption key name or serial number.

Example usage and output:

```
DLPCmd64 folder "C:\Secure Docs"
```

Virtual Disk Operations

The Command Line Tool can be used to perform mount and unmount operations on a virtual disk file.

Mount

Using the mount switch allows an encrypted virtual disk to be mounted for access.

Example usage:

```
DLPCmd64 mount documents.dlpvdisk
```

Global availability

When a virtual disk is mounted through the normal user interface or using the mount switch detailed above, it will only be available to access by processes running under the current Windows user context. This means that software which runs as another Windows user account will be unable to access the container. Please see here for further information: KB244 - Windows User context and encryption

In order to work around this the global mount switch can be used. Using this switch means **all users** on the system will be able to access the containers contents when it is mounted. This facility is only available through the command line tool and not the normal client UI.

To enable the global mount option simply add a *-g* switch to the command.

Example usage:

```
DLPCmd64 mount D:\Documents\secret.dlpvdisk -g
```

When mounting the file globally you will need to confirm the operation interactively. To avoid this, pass the additional *-i* switch.

Example usage:

```
DLPCmd64 mount D:\Documents\secret.dlpvdisk -g -i
```

Unmount

This command will unmount a mounted disk. You can use either the currently mounted drive letter or the path to the disk to indicate which disk you would like to unmount.

Example usage:

```
DLPCmd64 unmount X:
```

```
DLPCmd64 unmount D:\Documents\secret.dlpvdisk
```

Shredder Operations

The command line tool can be used to securely delete a file using the DESlock+ shredder.

Please note: using the shred option with securely erase the file and the data CANNOT be recovered.

Example usage:

```
DLPCmd64 shred mydocument.docx
```

This will shred the file using the default options.

> You will be prompted to confirm that you want to shred the file, and the file will be shredded using the Cryptographic Random Number method.

To bypass the confirmation and shred the file with no prompt, add the *-i* switch

Example usage:

```
DLPCmd64 shred mydocument.docx -i
```

To change the mode used to shred the file use one of the following switches:

-rand	*Shred the file using Cryptographic Random Number Data*
-gutmann	*Shred the file using the Gutmann algorithm*

-dode	*Shred the file using US DoD 5220.22-M (8-306. /E)*
-dodece	*Shred the file using US DoD 5220.22-M (8-306. /E, C and E)*

Example usage:

```
DLPCmd64 shred mydocument.docx -gutmann
```

Full Disk Encryption Status Operations

The Full Disk Encryption status of the system disks in the workstation can be displayed using the *query* command. The command can also be used to obtain a JSON formatted system report containing full details of the disks on the system and additional machine details.

Display status all disks

The full disk encryption status of all connected hard disks can be displayed using the *-l* switch as shown below:

Example usage and output:

```
DLPCmd64 query -l:
```

Display status of a specific drive or disk

You can display the encryption status of a specific drive by passing the drive letter as shown below:

Example usage:

```
DLPCmd64 query -l:C
```

Alternatively, to show the encryption status of a specific disk pass the disk number as shown below:

Example usage:

```
DLPCmd64 query -l:2
```

Exit codes

The query command call using the *-l* parameter have the following possible exit codes:

Exit code	Meaning
0-100	% encrypted (applies to disk or drive specific calls)
-101	Not encrypted
-102	Partially encrypted
-103	Fully encrypted
Other	Error

Save detailed system information

By supplying the *-f* switch and filename a JSON formatted file containing disk and system information will be produced.

Example usage:

```
DLPCmd64 query -f:C:\deslock_info.json
```

Help

To obtain help from the tool simply run without any parameters. Include the command for help about a specific command.

Related articles

KB244 - Windows User context and encryption

KB220 - What are the encryption size constraints?

Keywords : file encryption email text commandline dlpcmd mountfile mount file virtualdisk automation scheduled task user context shredder