SoftControl

DeCrypt 1.0.111

User guide

Dear user!

Safe'N'Sec Corporation thanks you for choosing SoftControl DeCrypt. Specialists of the company do their best to make sure our software both meets the highest requirements in a field of information protection and is easy use. We hope you find SoftControl DeCrypt helpful.

COPYRIGHT

LIABILITY LIMIT

Contents of the document may change without notice. Safe'N'Sec Corporation doesn't bear responsibility for inaccuracies and/or errors in this document, and possible damage associated with it.

Safe'N'Sec Corporation, 2018
Postal address:
127106 Russia, Moscow
Altufyevskoe shosse, 5/2
Safe'N'Sec Corporation
Tel:
+7 (495) 967-14-51
Fax:
+ 7 (495) 967-14-52
E-mails:
Customer service: support@safensoft.com
Sales team: sales@safensoft.com
Website: http://www.safensoft.com

Содержание

1. Introduction

1.1 Purpose

SoftControl DeCrypt encryption software is designed to encrypt the hard disks of Microsoft® Windows®-controlled self-service devices. SoftControl DeCrypt provides protection from the following types of attacks.

1. The violator steals the hard disk of a self-service device. The violator reverse engineers the contents of the disk in a lab, finds software vulnerabilities and subsequently carries out an attack on the self-service device.
2. The violator bypasses BIOS protection, loads the self-service device from an external drive and reverse engineers the contents of the hard disk.

When the encryption process runs, SoftControl DeCrypt reads out the parameters of all the devices connected to the computer. When the computer loads next time and no critical changes in the configuration are detected, the OS loads with the use of the device parameters. A change in computer configuration is considered critical if three or more devices have been modified or removed. Changing one or two devices is possible and is implemented with the help of Shamir's secret sharing algorithm.

If there is a critical change in the computer configuration, SoftControl DeCrypt prompts the user to enter the password he/she specified during disk encryption, to load the OS.

SoftControl DeCrypt is a client component and can operate both in stand-alone mode and in conjunction with SoftControl Service Center. For SoftControl DeCrypt to work with SoftControl Service Center, the SoftControl SysWatch client component should be installed on the computer along with SoftControl DeCrypt. SoftControl SysWatch transfers the encryption events to SoftControl Server.

For details on how to view SoftControl DeCrypt logs, see 'SoftControl Service Center administrator's guide'.

This product has been developed with the use of VeraCrypt source code that is licensed with VeraCrypt License. This license combines Apache License 2.0 and TrueCrypt License 3.0. A copy of the license is available in the application folder in the *VCLicense.txt* file.

1.2 Notational conventions and terms

1.2.1 Notational conventions

Table 1 lists notational conventions used in this document.

Table 1. Notational conventions

Notation example	Description
ℹ	An important information.
Condition	An execution condition, a note, or an example.
Update	– headers and acronyms; – names of buttons, links, menu items, and other program interface elements.
Control policy	– terms (definitions); – names of files and other objects; – messages displayed to user.
`C:\Program Files\SoftControl`	Paths to directories, files, or registry keys.
`%windir%\system32\msiexec.exe /i`	Source code, command and configuration file fragments.
<SoftControl DeCrypt installation directory>	Fields with specific names to be replaced with actual values.
Appendix 5	Links to internal resources (document sections) with a specific page number, or links to external resources (URL).

1.2.2 List of acronyms

This documents uses the following acronyms:

- **OS** – operating system;
- **GUI** – graphical user interface.

1.2.3 Glossary

Table 2. Glossary

Term	Description
Client host	A computer (a workstation, a server, a self-service terminal) with the installed SoftControl DeCrypt.
Boot loader	A component of the SoftControl DeCrypt encryption system. It loads the OS with the use of the device parameters, or with the use of the password (if loading with the device parameters failed).

2. Hardware and software requirements

2.1 SoftControl DeCrypt system requirements

Table 3. Minimal system requirements

OS	HDD free space
▪ Microsoft® Windows® 7 (64-bit) ▪ Microsoft® Windows® 8 (32-bit/64-bit) ▪ Microsoft® Windows® 8.1 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2003 (64-bit) ▪ Microsoft® Windows® Server 2008 64-bit) ▪ Microsoft® Windows® Server 2008 R2 ▪ Microsoft® Windows® Server 2012 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2012 R2 (32-bit/64-bit) ▪ Microsoft® Windows® 10 (32-bit/64-bit) ▪ Microsoft® Windows® Server 2016 (32-bit/64-bit)	100MB + extra 10MB in the UEFI partition

Additional requirements:

- BIOS type: UEFI. We recommend that you disable the **SecureBoot** option.
- The hard disk should use GPT (GUID Partition Table). Unallocated space should be available in the beginning sector (at least 32KB). See also information in Appendix 37.

3. Installing SoftControl DeCrypt

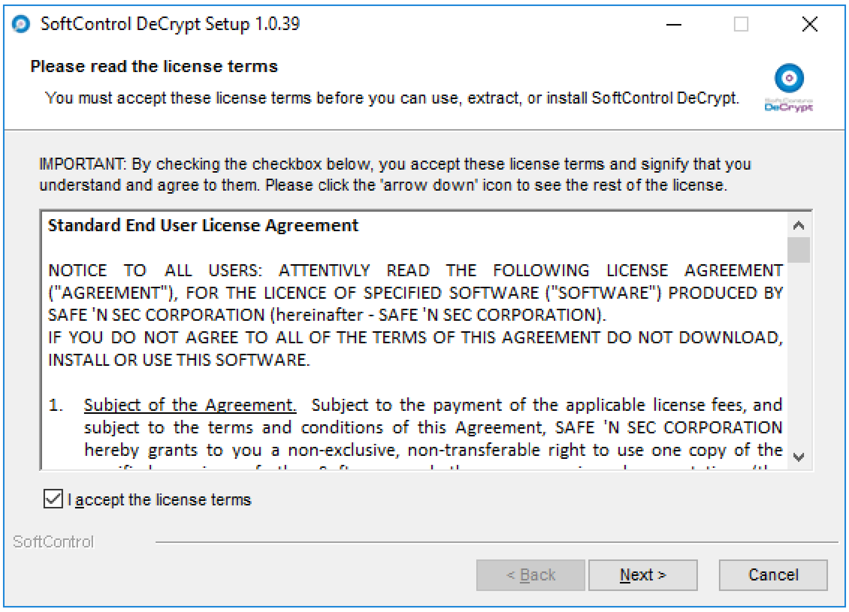
You can install SoftControl DeCrypt in the following ways:

- standard mode (via GUI)[7];
- silent mode[9].

3.1 Installing in standard mode

1) Run the *SoftControl DeCrypt Setup 1.0.111 .exe* installation package.

2) If you accept the terms, select **I accept the license** and click **Next** (fig. License agreement[7]).



SoftControl DeCrypt Setup 1.0.39

Please read the license terms

You must accept these license terms before you can use, extract, or install SoftControl DeCrypt.

IMPORTANT: By checking the checkbox below, you accept these license terms and signify that you understand and agree to them. Please click the 'arrow down' icon to see the rest of the license.

Standard End User License Agreement

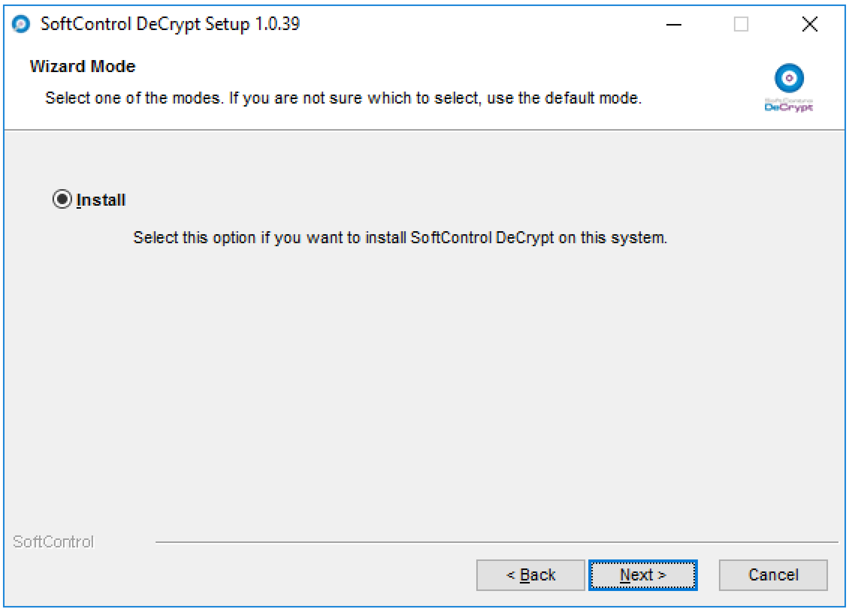
NOTICE TO ALL USERS: ATTENTIVLY READ THE FOLLOWING LICENSE AGREEMENT ("AGREEMENT"), FOR THE LICENCE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY SAFE 'N SEC CORPORATION (hereinafter - SAFE 'N SEC CORPORATION).
IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

1. Subject of the Agreement. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, SAFE 'N SEC CORPORATION hereby grants to you a non-exclusive, non-transferable right to use one copy of the

☑ I accept the license terms

Figure 1. License agreement

3) Select the required option in the **Wizard Mode** window and click **Next** (fig. Selecting the installation option[7]).



SoftControl DeCrypt Setup 1.0.39

Wizard Mode

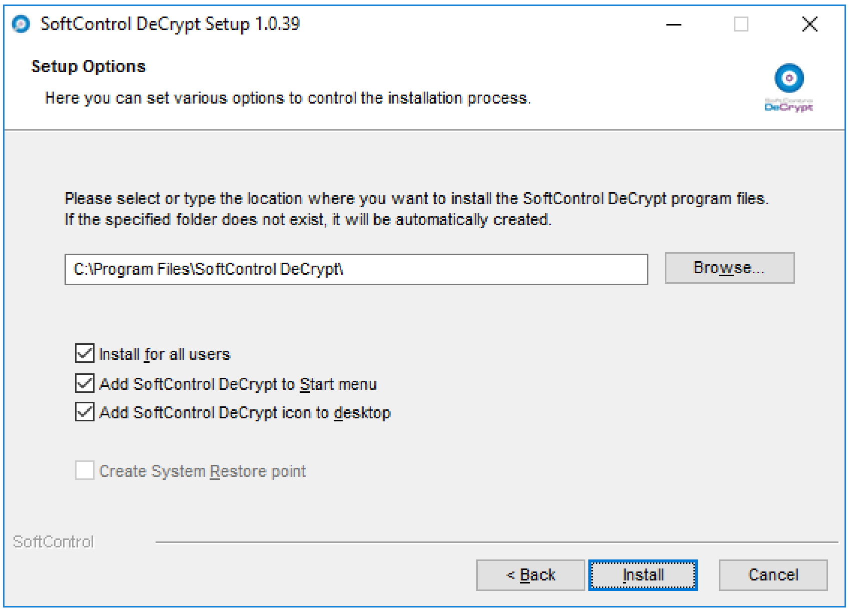
Select one of the modes. If you are not sure which to select, use the default mode.

● **Install**

Select this option if you want to install SoftControl DeCrypt on this system.

Figure 2. Selecting the installation option

4) Select a directory to install SoftControl DeCrypt to (with the help of the **Browse** button) and click **Next** (fig. Installation path 8).



SoftControl DeCrypt Setup 1.0.39

Setup Options

Here you can set various options to control the installation process.

Please select or type the location where you want to install the SoftControl DeCrypt program files.
If the specified folder does not exist, it will be automatically created.

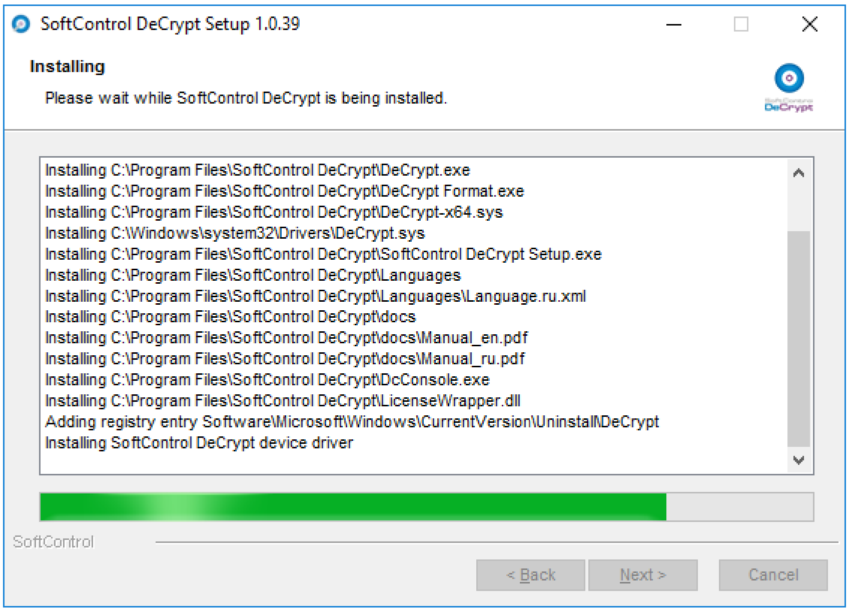
C:\Program Files\SoftControl DeCrypt\

☑ Install for all users
☑ Add SoftControl DeCrypt to Start menu
☑ Add SoftControl DeCrypt icon to desktop

□ Create System Restore point

Figure 3. Installation path

5) Wait until installation completes (fig. Installation progress 8).


SoftControl DeCrypt Setup 1.0.39

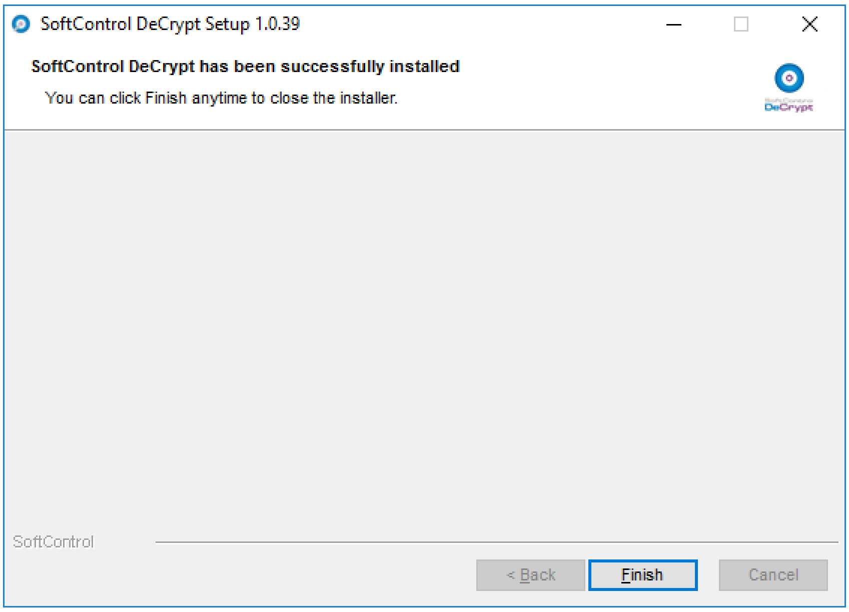
Installing

Please wait while SoftControl DeCrypt is being installed.

```
Installing C:\Program Files\SoftControl DeCrypt\DeCrypt.exe
Installing C:\Program Files\SoftControl DeCrypt\DeCrypt Format.exe
Installing C:\Program Files\SoftControl DeCrypt\DeCrypt-x64.sys
Installing C:\Windows\system32\Drivers\DeCrypt.sys
Installing C:\Program Files\SoftControl DeCrypt\SoftControl DeCrypt Setup.exe
Installing C:\Program Files\SoftControl DeCrypt\Languages
Installing C:\Program Files\SoftControl DeCrypt\Languages\Language.ru.xml
Installing C:\Program Files\SoftControl DeCrypt\docs
Installing C:\Program Files\SoftControl DeCrypt\docs\Manual_en.pdf
Installing C:\Program Files\SoftControl DeCrypt\docs\Manual_ru.pdf
Installing C:\Program Files\SoftControl DeCrypt\DcConsole.exe
Installing C:\Program Files\SoftControl DeCrypt\LicenseWrapper.dll
Adding registry entry Software\Microsoft\Windows\CurrentVersion\Uninstall\DeCrypt
Installing SoftControl DeCrypt device driver
```

Figure 4. Installation progress

6) After the **SoftControl DeCrypt has been successfully installed** message is displayed, click **Finish** (fig. Installation completes 9).


SoftControl DeCrypt Setup 1.0.39

SoftControl DeCrypt has been successfully installed

You can click Finish anytime to close the installer.

Figure 5. Installation completes

3.2 Installing in silent mode

Important: All steps require administrator privileges.

1) Copy the *SoftControl DeCrypt Setup 1.0.111 .exe* installation package to a folder on the client host.

2) Run Windows command prompt and enter the following command:

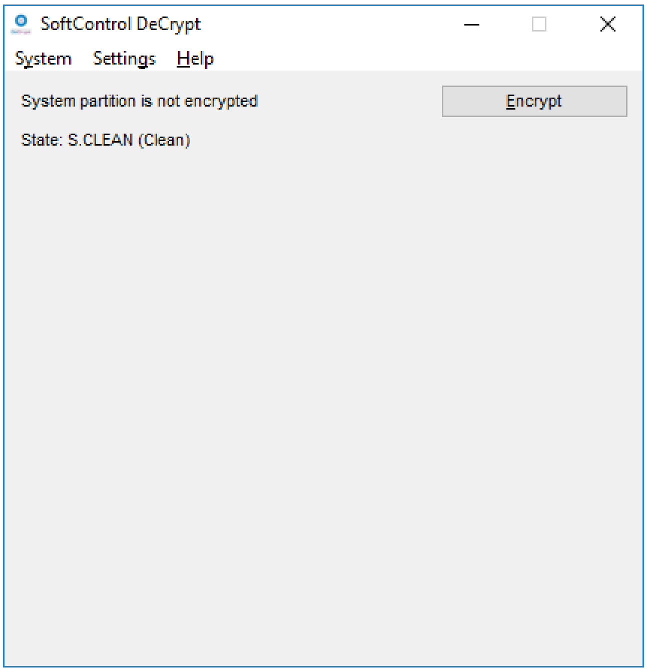
```
"<folder with the installation package>\SoftControl DeCrypt Setup 1.0.111 .exe" /q [/folder
"<installation folder>"]
```

If the optional `/folder` parameter is not used, the default installation folder for SoftControl DeCrypt is `C:\Program Files\SoftControl DeCrypt`.

4. Working with SoftControl DeCrypt

This section contains instructions on how to work with the main SoftControl DeCrypt functions.

SoftControl DeCrypt GUI is shown in fig. Elements of the program GUI 11 .



System partition is not encrypted

State: S.CLEAN (Clean)

Figure 6. Elements of the program GUI

Table 4 lists the menu commands.

Table 4. SoftControl DeCrypt menu commands

Command	Action
Encrypt system partition/drive...	Run the encryption of the hard disk or system volume.
Decrypt system partition/drive	Run the decryption of the hard disk or system volume.
Resume interrupted process	Resume the interrupted encryption or decryption process.
Remove boot loader	Remove the encryption system loader without removing SoftControl DeCrypt (system reboot is required).
Change password...	Change the password that is used to load the system in case there are critical changes in the set of devices.
Update devices...	Add new devices to the set of devices.
Language...	Change GUI language.
User's Guide	Invoke user guide.

Table 5 lists the system statuses.

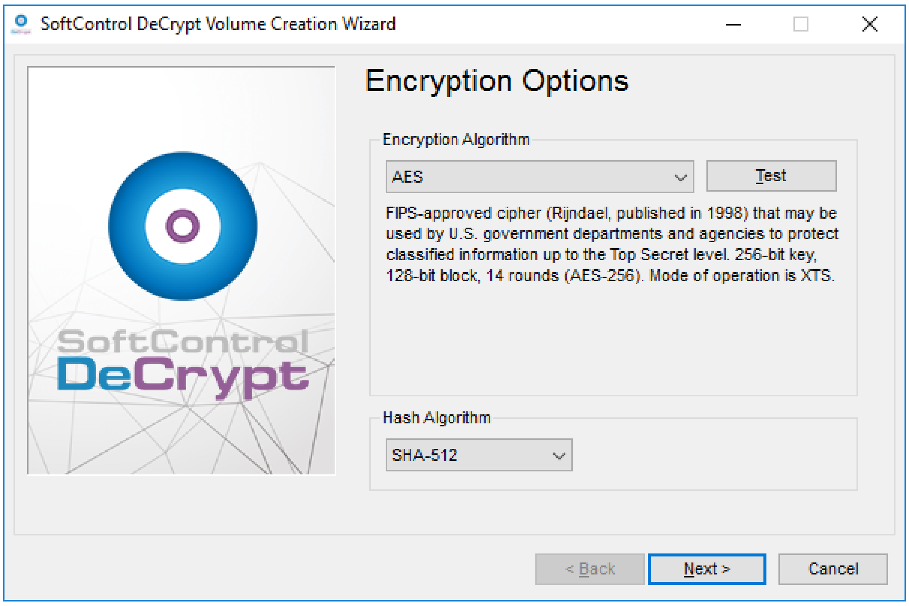
Table 5. SoftControl DeCrypt statuses

State	Description
S.CLEAN (Clean)	SoftControl DeCrypt is installed on the client host but the disk does not contain the boot loader.
S.INST (Installed)	The boot loader is installed but have not run yet (the client host has not rebooted).
S.MNT (Mounted)	The boot loader is installed, the client host has rebooted, but disk encryption has not yet run.
S.PART_ENC (Partially encrypted)	Disk encryption or decryption is in progress.
S.FULL_ENC (Fully encrypted)	Disk is encrypted.

4.1 Encrypting system volume

Click **Encrypt** in the main SoftControl DeCrypt window (fig. Elements of the program GUI[11]).

In the displayed window, select **Encryption algorithm** and **Hash algorithm** from the drop-down lists and click **Next** (fig. Encryption options[12]).



Encryption Options

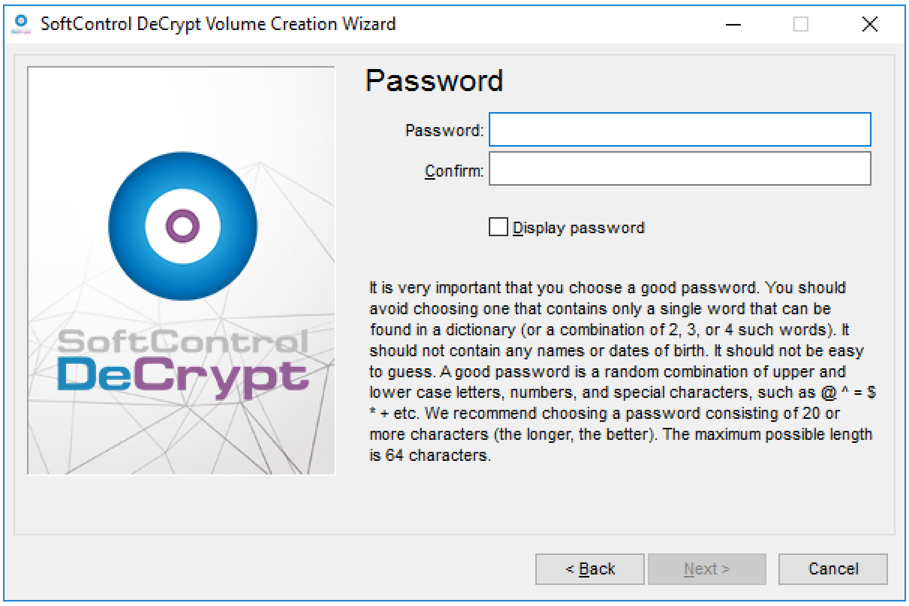
Encryption Algorithm: AES

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

Hash Algorithm: SHA-512

Figure 7. Encryption options

Set the **Password** and confirm it (fig. Specifying the password[12]).



Password

Password:

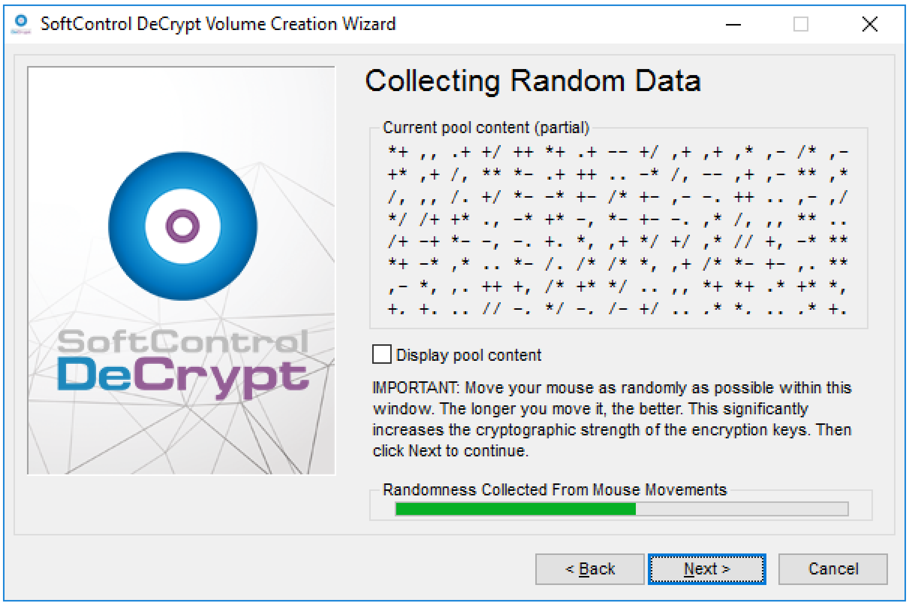
Confirm:

□ Display password

It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ ^ = $ * + etc. We recommend choosing a password consisting of 20 or more characters (the longer, the better). The maximum possible length is 64 characters.

Figure 8. Specifying the password

In the next window, SoftControl DeCrypt collects random data from the mouse movements. Move your mouse within the window. We recommend that you do so until the progress bar turns green; then click **Next** (fig. Collecting random data [13]).



Collecting Random Data

Current pool content (partial)

```
*+ ,, .+ +/ ++ *+ .+ -- +/ ,+ ,+ ,* ,- /* ,-
+* ,+ /, ** *- .+ ++ .. -* /, -- ,+ ,- ** ,*
/, ,, /. +/ *- -* +- /* +- ,- -. ++ .. ,- ,/
*/ /+ +* ., -* +* -, *- +- -. ,* /, ,, ** ..
/+ -+ *- -, -. +. *, ,+ */ +/ ,* // +, -* **
*+ -* ,* .. *- /. /* /* *, ,+ /* *- +- ,. **
,- *, ,. ++ +, /* +* */ .. ,, *+ *+ .* +* *,
+. +. .. // -. */ -. /- +/ .. .* *. .. .* +.
```

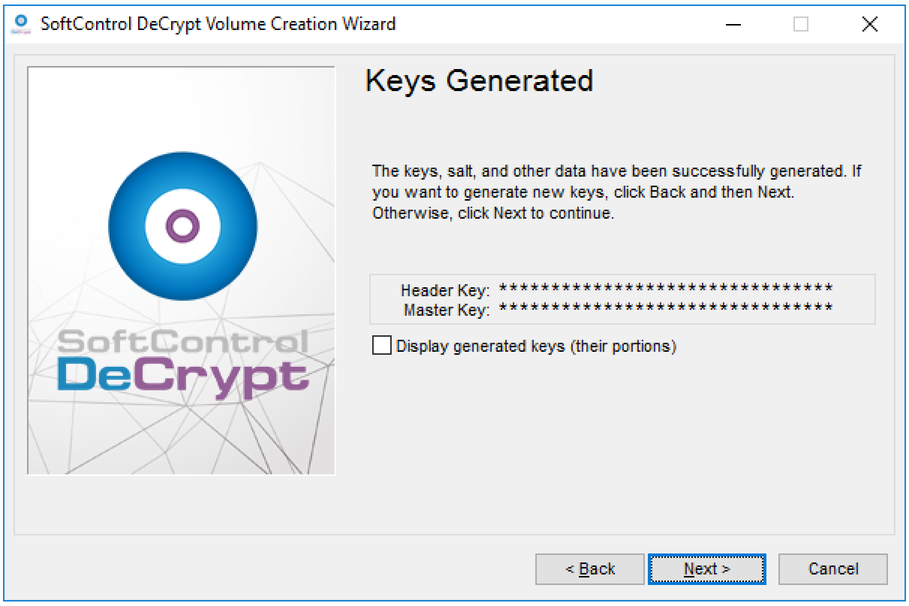
□ Display pool content

IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Next to continue.

Randomness Collected From Mouse Movements

Figure 9. Collecting random data

To view the keys in the next window (fig. Generated keys [13]), tick off **Display generated keys (their portions)**.



SoftControl DeCrypt Volume Creation Wizard

Keys Generated

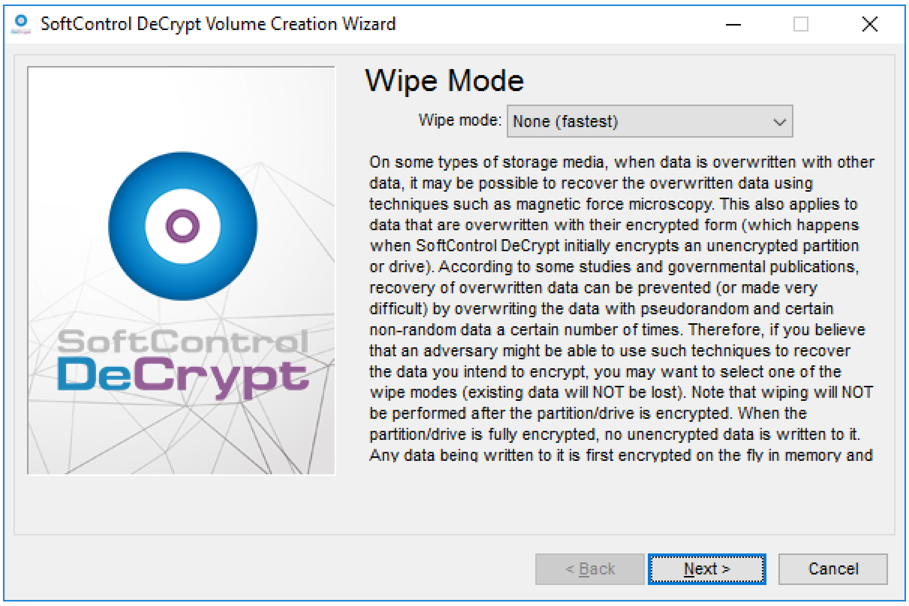
The keys, salt, and other data have been successfully generated. If you want to generate new keys, click Back and then Next. Otherwise, click Next to continue.

Header Key: ********************************
Master Key: ********************************

□ Display generated keys (their portions)

Figure 10. Generated keys

Select the **Wipe mode** from the drop-down list (fig. Selecting wipe mode 14).



SoftControl DeCrypt Volume Creation Wizard

Wipe Mode

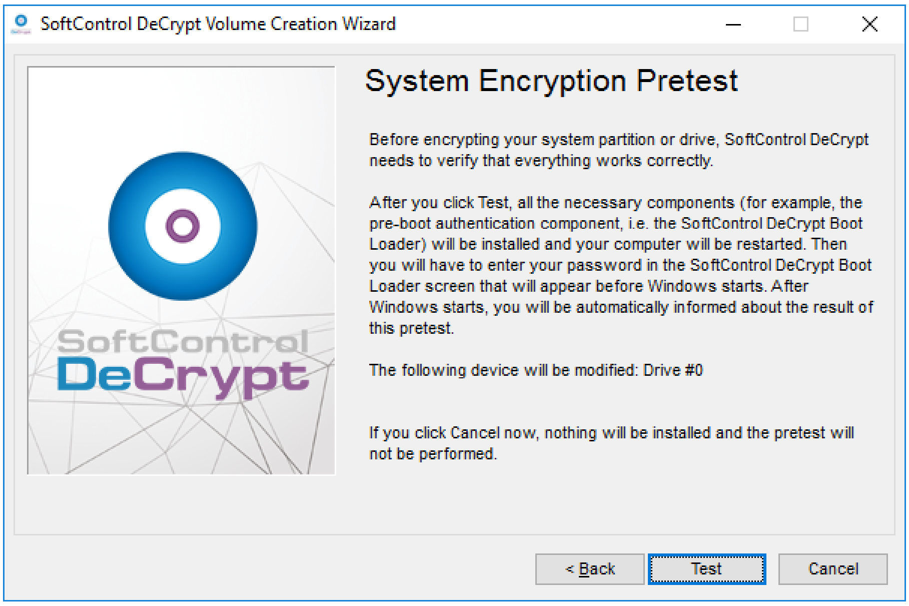
Wipe mode: None (fastest)

On some types of storage media, when data is overwritten with other data, it may be possible to recover the overwritten data using techniques such as magnetic force microscopy. This also applies to data that are overwritten with their encrypted form (which happens when SoftControl DeCrypt initially encrypts an unencrypted partition or drive). According to some studies and governmental publications, recovery of overwritten data can be prevented (or made very difficult) by overwriting the data with pseudorandom and certain non-random data a certain number of times. Therefore, if you believe that an adversary might be able to use such techniques to recover the data you intend to encrypt, you may want to select one of the wipe modes (existing data will NOT be lost). Note that wiping will NOT be performed after the partition/drive is encrypted. When the partition/drive is fully encrypted, no unencrypted data is written to it. Any data being written to it is first encrypted on the fly in memory and

Figure 11. Selecting wipe mode

Enabling the wipe mode increases the disk encryption time significantly.

After you click **Next** in the **Wipe mode** window (see above 14), SoftControl DeCrypt suggests running a pretest to make sure the system is ready for encryption. The SoftControl DeCrypt boot loader is installed during pretest (fig. Running the pretest 14).



System Encryption Pretest

Before encrypting your system partition or drive, SoftControl DeCrypt needs to verify that everything works correctly.

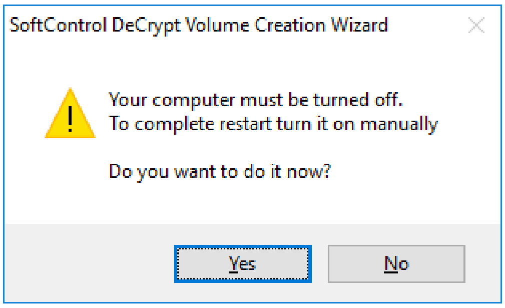
After you click Test, all the necessary components (for example, the pre-boot authentication component, i.e. the SoftControl DeCrypt Boot Loader) will be installed and your computer will be restarted. Then you will have to enter your password in the SoftControl DeCrypt Boot Loader screen that will appear before Windows starts. After Windows starts, you will be automatically informed about the result of this pretest.

The following device will be modified: Drive #0

If you click Cancel now, nothing will be installed and the pretest will not be performed.

Figure 12. Running the pretest

Click **Yes** in the window that asks you to turn off the client host. To run the pretest, you need to boot the computer manually (fig. Turning off the computer[15]).

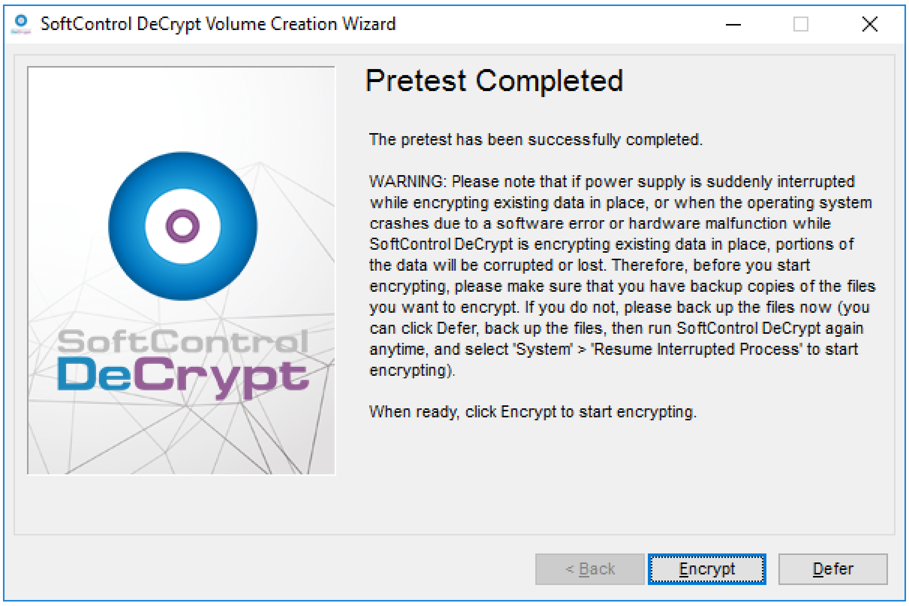


Your computer must be turned off.
To complete restart turn it on manually

Do you want to do it now?

Figure 13. Turning off the computer

After the client host reboots, SoftControl DeCrypt displays a message that the pretest has completed (fig. Pretest completed[15]).



Pretest Completed

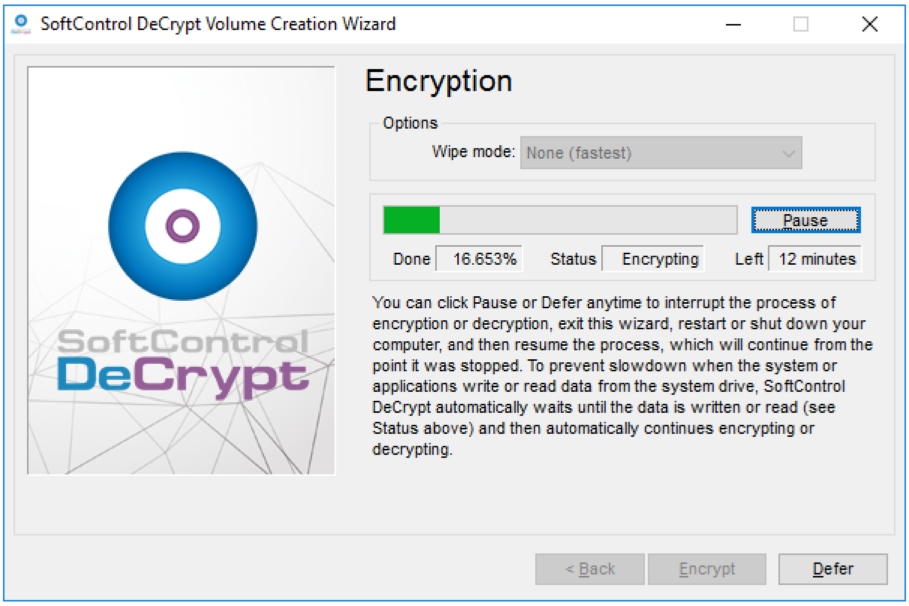
The pretest has been successfully completed.

WARNING: Please note that if power supply is suddenly interrupted while encrypting existing data in place, or when the operating system crashes due to a software error or hardware malfunction while SoftControl DeCrypt is encrypting existing data in place, portions of the data will be corrupted or lost. Therefore, before you start encrypting, please make sure that you have backup copies of the files you want to encrypt. If you do not, please back up the files now (you can click Defer, back up the files, then run SoftControl DeCrypt again anytime, and select 'System' > 'Resume Interrupted Process' to start encrypting).

When ready, click Encrypt to start encrypting.

Figure 14. Pretest completed

Click **Encrypt** to run disk encryption. The **Encryption** window displays the progress bar and the remaining time (fig. Disk encryption (16)).



Encryption

Options

Wipe mode: None (fastest)

Done 16.653% Status Encrypting Left 12 minutes

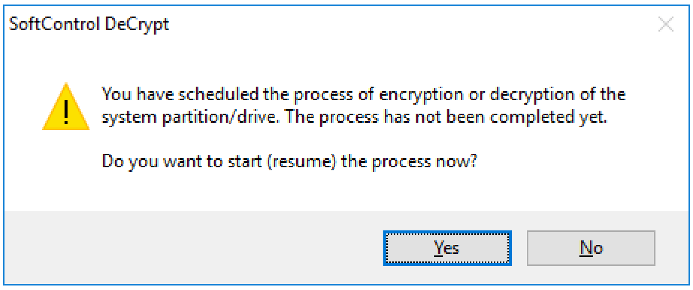
You can click Pause or Defer anytime to interrupt the process of encryption or decryption, exit this wizard, restart or shut down your computer, and then resume the process, which will continue from the point it was stopped. To prevent slowdown when the system or applications write or read data from the system drive, SoftControl DeCrypt automatically waits until the data is written or read (see Status above) and then automatically continues encrypting or decrypting.

Figure 15. Disk encryption

You can interrupt the encryption process if necessary by clicking **Pause**, and run it again later by clicking **Resume**.

To run the encryption process later, click **Defer**. To resume the process, select **Resume interrupted process** in the main SoftControl DeCrypt window (table SoftControl DeCrypt menu commands (11)).

Note. If encryption has been interrupted, SoftControl DeCrypt displays the following message after the client host reboots (fig. Resuming disk encryption (16)).



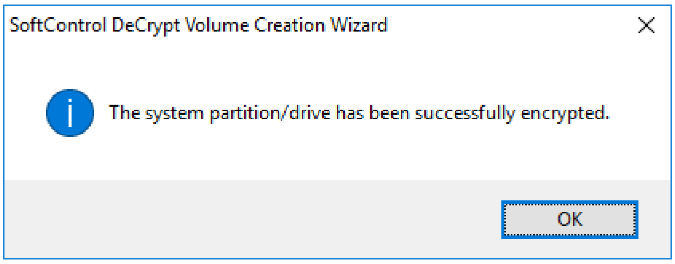
SoftControl DeCrypt

You have scheduled the process of encryption or decryption of the system partition/drive. The process has not been completed yet.

Do you want to start (resume) the process now?

Рисунок 16. Resuming disk encryption

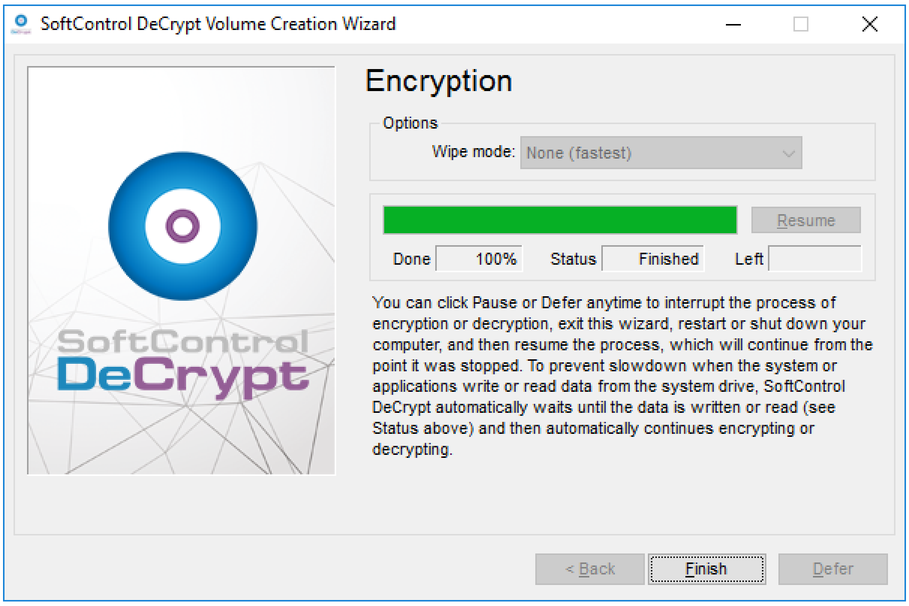
Click **OK** in the displayed window (fig. Encryption completed 17); then click **Finish** to complete the process (fig. Disk is encrypted 17).



SoftControl DeCrypt Volume Creation Wizard

The system partition/drive has been successfully encrypted.

Figure 17. Encryption completed



SoftControl DeCrypt Volume Creation Wizard

Encryption

Options

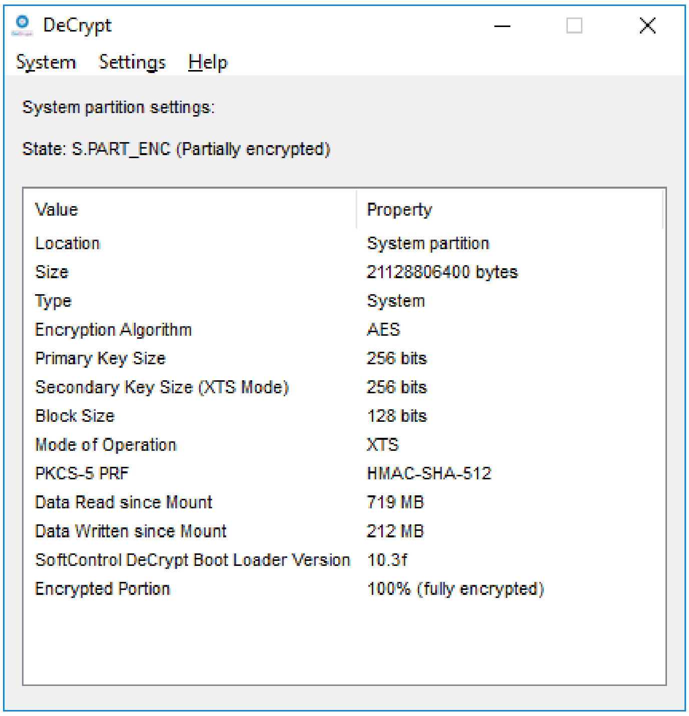
Wipe mode: None (fastest)

Done 100% Status Finished Left

You can click Pause or Defer anytime to interrupt the process of encryption or decryption, exit this wizard, restart or shut down your computer, and then resume the process, which will continue from the point it was stopped. To prevent slowdown when the system or applications write or read data from the system drive, SoftControl DeCrypt automatically waits until the data is written or read (see Status above) and then automatically continues encrypting or decrypting.

Figure 18. Disk is encrypted

When you run SoftControl DeCrypt next time, the main window displays the encryption parameters (fig. Encryption parameters 17).



System partition settings:

State: S.PART_ENC (Partially encrypted)

Value	Property
Location	System partition
Size	21128806400 bytes
Type	System
Encryption Algorithm	AES
Primary Key Size	256 bits
Secondary Key Size (XTS Mode)	256 bits
Block Size	128 bits
Mode of Operation	XTS
PKCS-5 PRF	HMAC-SHA-512
Data Read since Mount	719 MB
Data Written since Mount	212 MB
SoftControl DeCrypt Boot Loader Version	10.3f
Encrypted Portion	100% (fully encrypted)

Figure 19. Encryption parameters

4.2 Modifying the set of connected devices

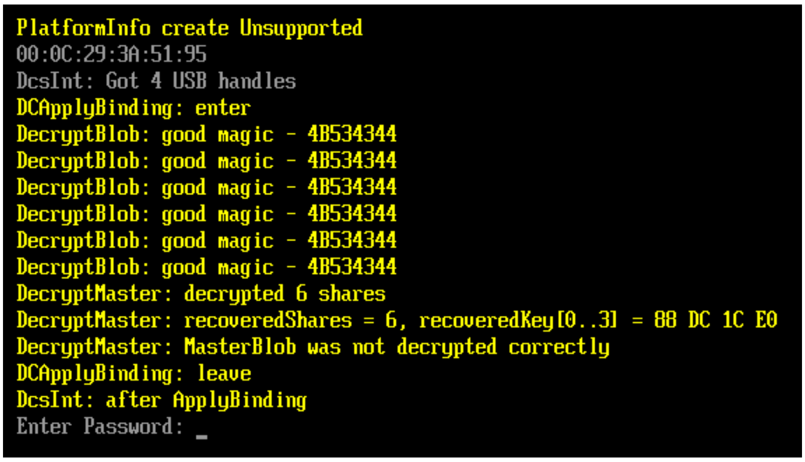
When the encryption process runs, SoftControl DeCrypt reads out the parameters of the following devices:

- MAC addresses of the network cards;
- VID, PID and serial numbers of USB drives;
- BIOS (information about the processor in the motherboard).

The minimum number of devices that SoftControl DeCrypt supports is two (the client host should have network cards or USB drives connected to it). The list of devices that SoftControl DeCrypt has read out is logged to the event log.

When a device has been changed (removed), SoftControl DeCrypt allows the encrypted disk to load. The corresponding message is added to the event log. When any two devices from the set has been changed (removed), SoftControl DeCrypt allows the encrypted disk to load as well. The message about a critical change in the set of devices is added to the event log.

If more than two devices has been changed (removed), SoftControl DeCrypt prompts you to enter the password specified during disk encryption, to load the client host (fig. Requesting the password when loading the client host 18).



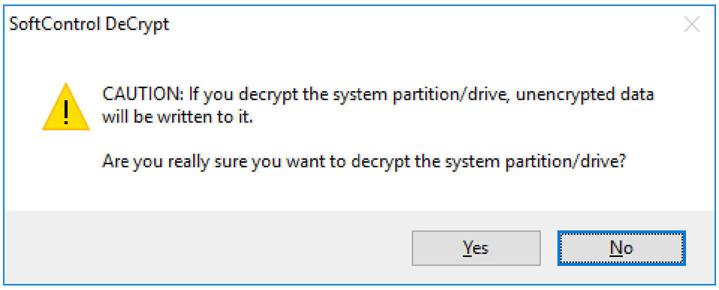
```
PlatformInfo create Unsupported
00:0C:29:3A:51:95
DcsInt: Got 4 USB handles
DCApplyBinding: enter
DecryptBlob: good magic - 4B534344
DecryptBlob: good magic - 4B534344
DecryptBlob: good magic - 4B534344
DecryptBlob: good magic - 4B534344
DecryptBlob: good magic - 4B534344
DecryptBlob: good magic - 4B534344
DecryptMaster: decrypted 6 shares
DecryptMaster: recoveredShares = 6, recoveredKey[0..3] = 88 DC 1C E0
DecryptMaster: MasterBlob was not decrypted correctly
DCApplyBinding: leave
DcsInt: after ApplyBinding
Enter Password: _
```

Figure 20. Requesting the password when loading the client host

When you run disk encryption, SoftControl DeCrypt reads out the parameters of the devices detected during client host loading. If the critical number of devices has been disconnected after the encryption, the client host continues to work. After reboot, however, SoftControl DeCrypt asks for the password to load the client host.

4.3 Decrypting system volume

In the main SoftControl DeCrypt window, select the **Decrypt system partition/drive** command from the **System** menu (table SoftControl DeCrypt menu commands (11)). Select **Yes** in the message with the warning (fig. Confirming disk decryption (19)) and wait till the process completes (fig. The disk is decrypted (20)).



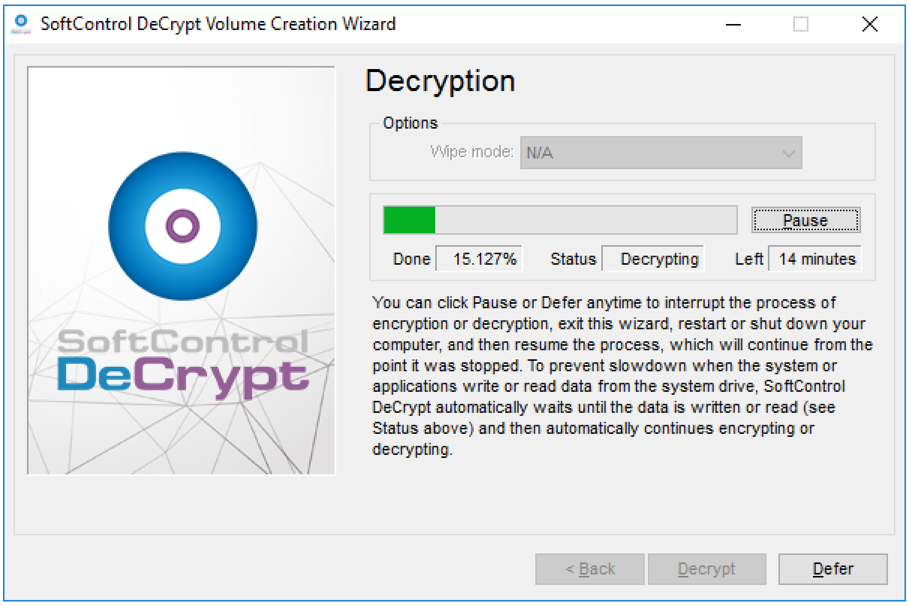
SoftControl DeCrypt

CAUTION: If you decrypt the system partition/drive, unencrypted data will be written to it.

Are you really sure you want to decrypt the system partition/drive?

Figure 21. Confirming disk decryption

As with the encryption (see section Encrypting system volume (16)), you can interrupt or postpone the process by clicking **Pause** or **Defer** (fig. Decrypting the disk (19)).



Decryption

Options

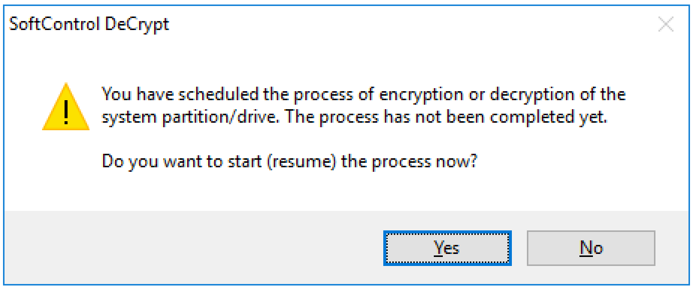
Wipe mode: N/A

Done 15.127% Status Decrypting Left 14 minutes

You can click Pause or Defer anytime to interrupt the process of encryption or decryption, exit this wizard, restart or shut down your computer, and then resume the process, which will continue from the point it was stopped. To prevent slowdown when the system or applications write or read data from the system drive, SoftControl DeCrypt automatically waits until the data is written or read (see Status above) and then automatically continues encrypting or decrypting.

Figure 22. Decrypting the disk

Note. If decryption has been interrupted, SoftControl DeCrypt displays the following message after the client host reboots (fig. Resuming disk decryption 20).

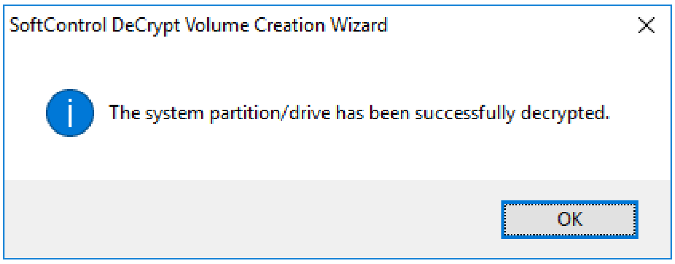


You have scheduled the process of encryption or decryption of the system partition/drive. The process has not been completed yet.

Do you want to start (resume) the process now?

Рисунок 23. Resuming disk decryption

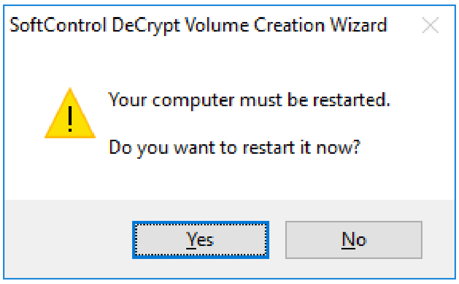
Click **OK** in the displayed window (fig. The disk is decrypted 20)



The system partition/drive has been successfully decrypted.

Figure 24. The disk is decrypted

Click **Yes** In the dialog box that suggests system reboot. The client host then reboots to complete the process (fig. Requesting system reboot 20).



SoftControl DeCrypt Volume Creation Wizard

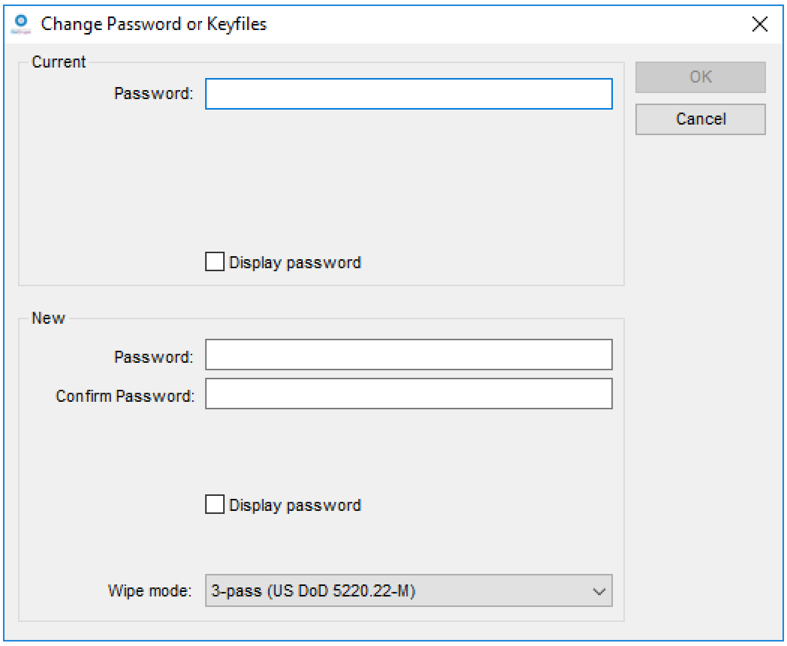
Your computer must be restarted.

Do you want to restart it now?

Figure 25. Requesting system reboot

4.4 Changing the password

To change the password you specified when you ran encryption, select **Change password...** from the **System** menu (fig. Changing the password[21]).



Change Password or Keyfiles

Current

Password:

□ Display password

New

Password:

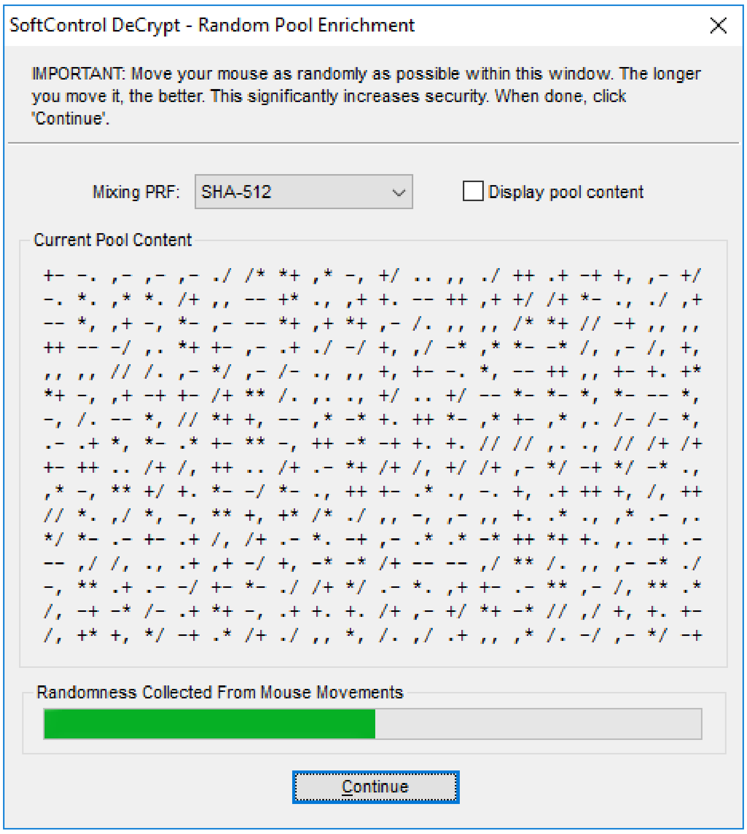
Confirm Password:

□ Display password

Wipe mode: 3-pass (US DoD 5220.22-M)

Figure 26. Changing the password

Enter the current password, enter a new password, confirm it, and click **OK**. In the **Random pool enrichment** window, move your mouse to collect random data (fig. Collecting random data to change the password[21]), just as you did to generate keys for encryption (see fig. Collecting random data[13]).



IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases security. When done, click 'Continue'.

Mixing PRF: SHA-512

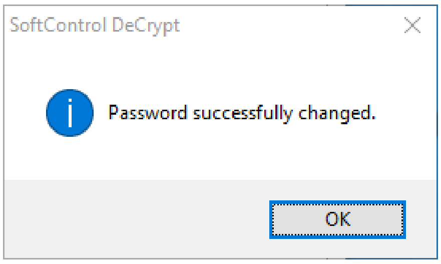
□ Display pool content

Current Pool Content

```
+- -. ,- ,- ,- ./ /* *+ ,* -, +/ .. ,, ./ ++ .+ -+ +, ,- +/
-. *. ,* *. /+ ,, -- +* ., ,+ +. -- ++ ,+ +/ /+ *- ., ./ ,+
-- *, ,+ -, *- ,- -- *+ ,+ *+ ,- /. ,, ,, /* *+ // -+ ,, ,,
++ -- -/ ,. *+ +- ,- .+ ./ -/ +, ,/ -* ,* *- -* /, ,- /, +,
,, ,, // /. ,- */ ,- /- ., ,, +, +- -. *, -- ++ ,, +- +. +*
*+ -, ,+ -+ +- /+ ** /. ,. ., +/ .. +/ -- *- *- *, *- -- *,
-, /. -- *, // *+ +, -- ,* -* +. ++ *- ,* +- ,* ,. /- /- *,
.- .+ *, *- .* +- ** -, ++ -* -+ +. +. // // ,. ., // /+ /+
+- ++ .. /+ /, ++ .. /+ .- *+ /+ /, +/ /+ ,- */ -+ */ -* .,
,* -, ** +/ +. *- -/ *- ., ++ +- .* ., -. +, .+ ++ +, /, ++
// *. ,/ *, -, ** +, +* /* ./ ,, -, ,- ,, +. .* ., ,* .- ,.
*/ *- .- +- .+ /, /+ .- *. -+ ,- .* .* -* ++ *+ +. ,. -+ .-
-- ,/ /, ., .+ ,+ -/ +, -* -* /+ -- -- ,/ ** /. ,, ,- -* ./
-, ** .+ .- -/ +- *- ./ /+ */ .- *. ,+ +- .- ** ,- /, ** .*
/, -+ -* /- .+ *+ -, .+ +. +. /+ ,- +/ *+ -* // ,/ +, +. +-
/, +* +, */ -+ .* /+ ./ ,, *, /. ,/ .+ ,, ,* /. -/ ,- */ -+
```

Randomness Collected From Mouse Movements

Figure 27. Collecting random data to change the password



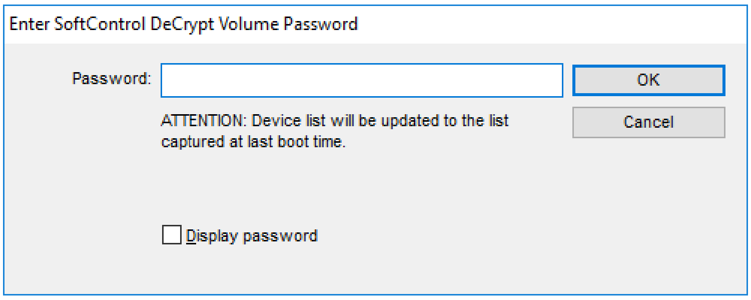
Password successfully changed.

Figure 28. Password has been changed

To complete the process, click **Continue** (see above[21]) and **OK** (fig. Password has been changed[22]).

4.5 Updating the list of devices

You can modify the device list created during disk encryption, without decrypting the disk. To do so, change the required devices, select **Update devices...** in the **System** menu, and enter the password (fig. Entering the password to change the connected devices 23).



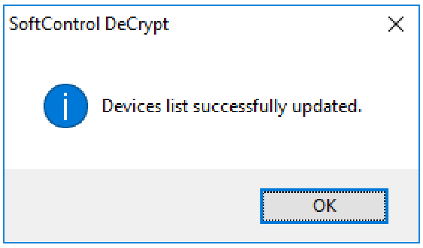
Enter SoftControl DeCrypt Volume Password

Password:

ATTENTION: Device list will be updated to the list captured at last boot time.

Figure 29. Entering the password to change the connected devices

SoftControl DeCrypt searches for all supported devices detected during OS loading, reads out their parameters and displays a message that the process has completed (fig. The list of devices is updated 23).



SoftControl DeCrypt

Devices list successfully updated.

Figure 30. The list of devices is updated

4.6 Using Command Prompt

You can perform all operations described in sections above from the Windows Command Prompt as follows.

```
"<SoftControl DeCrypt installation folder>\DcConsole.exe" /<command> [<parameters>]
```

Table 6 lists available commands and their parameters.

Important: all steps require administrator privileges.

Table 6. SoftControl DeCrypt command line parameters

Command/Parameter	Action/Possible values

`/boot-prepare (/newpass` *password*`|`
`/newpassfile` *file_with_password*`|`
`/cryptpass` *encrypted_data_block*`|`
`/cryptpassfile`
file_with_encrypted_data_block`) [/ha 1|2|3|4|5] [/ea 1|2|3|4|6|7|8|9|10|11]`
	Install the boot loader.
	You can set the disk encryption password in the following ways.
	a) specify it explicitly with the help of the `/newpass` parameter;
	b) write it to a file with any extension and ASCII encoding and specify the name of the file with the help of the `/newpassfile` parameter.
	The password should contains letters a-z, A-Z, figures 0-1 and special characters !@#$%^&*()_+.
	c) specify *encrypted_data_block* (generated by DcUtil.exe 28), with the help of the `/cryptpass` parameter.
	d) specify *file_with_encrypted_data_block* (generated by DcUtil.exe 28), with the help of the `/cryptpassfile` parameter.
	
	If hash algorithm and encryption algorithm are not specified, the default values specified below are used.
	The values for hash algorithm (the `/ha` parameter):
	1 – SHA-512 (default)
	2 – Whirlpool
	3 – SHA-256
	4 – RIPEMD-160
	5 – Streebog
	The values for encryption algorithm (the `/ea` parameter):
	1 – AES (default)
	2 – Serpent
	3 – Twofish
	4 – Camellia
	5 – (reserved)
	6 – Kuznyechik
	7 – Twofish+AES
	8 – Serpent+Twofish+AES
	9 – AES+Serpent
	10 – AES+Twofish+Serpent
	11 – Serpent+Twofish

`/disk-enc`	Start disk/partition encryption. If encryption has been interrupted (for example, because of the client host reboot or shutdown), the process resumes automatically after the client host boots.
`/disk-dec [/noreboot]`	Start disk/partition decryption. If decryption has been interrupted (for example, because of the client host reboot or shutdown), the process resumes automatically after the client host boots. If you use the `/noreboot` parameter, the client host does not reboot after decryption completes.
`/lic-set` *license_key*	Activate the license key you obtained when you purchased SoftControl DeCrypt.

Command/Parameter	Action/Possible values
/pw-change (/currpass *current_password*| /currpassfile *file_with_current_password*) (/newpass *new_password*| /newpassfile *file_with_new_password*)	Change the *current_password* that is used to load the system if there is a critical change in the set of devices. You can specify the current explicitly (with the help of the /currpass parameter) or through the *file_with_current_password*. You can specify the new password explicitly (with the help of the /newpass parameter) or through the *file_with_new_password*.
/pw-change (/cryptpass *encrypted_data_block*| /cryptpassfile *file_with_encrypted_data_block*)	Change the password that is used to load the system if there is a critical change in the set of devices. You can specify both current and new passwords with the help of a single *encrypted_data_block*, or with the help of the *file_with_encrypted_data_block*.
/dev-change (/currpass *current_password*| /currpassfile *file_with_current_password*| /cryptpass *encrypted_data_block*| /cryptpassfile *file_with_encrypted_data_block*)	Create a new list of devices that are used for system loading. You can specify the password explicitly (with the help of the /currpass parameter), through the *file_with_current_password*, through the *encrypted_data_block*, or through the *file_with_encrypted_data_block*.
/state	Display current SoftControl DeCrypt status.
/dev-get (/currpass *current_password*| /currpassfile *file_with_current_password*| /cryptpass *encrypted_data_block*| /cryptpassfile *file_with_encrypted_data_block*)	Load information about the connected devices to the event log. You can specify the password explicitly (with the help of the /currpass parameter), through the *file_with_current_password*, through the *encrypted_data_block*, or through the *file_with_encrypted_data_block*.
/boot-clear	Remove the boot loader from the client host.
/stop	Stop disk/partition encryption or decryption. The process resumes automatically after the client host reboots.
/seed-get	Get a data block for password transfer. You can only use the generated value once. After you run any command on the computer with the installed SoftControl DeCrypt or after you reboot this computer, you need to run /seed-get once more.

Example: You can run complete SoftControl DeCrypt installation procedure with the help of the following installation scripts (.cmd or .bat files).

To install SoftControl DeCrypt and the boot loader:

```
"<folder with the installation package>\SoftControl DeCrypt Setup 1.0.111 .exe" /q [/folder
"<installation folder>"]
"<SoftControl DeCrypt installation folder>\DcConsole.exe" /boot-prepare /newpassfile
<file_with_password>
```

If the /boot-prepare command uses the /newpass parameter, the password for disk encryption and decryption is stored unprotected in the script file or in the event log.

To check system status and run the encryption (after the client host reboots):

```
"<SoftControl DeCrypt installation folder>\DcConsole.exe" /state
"<SoftControl DeCrypt installation folder>\DcConsole.exe" /disk-enc
```

The `/disk-enc` command runs (i.e. the encryption process starts) only if the `/state` command in the script above has returned `S.MNT (Mounted)`. Otherwise, the script displays an error.

You can check the status of the encryption process with the help of the `/state` command. (When the encryption completes, the command returns `S.FULL_ENC (Fully encrypted)`.)

4.7 Reports

SoftControl DeCrypt enables logging the events and the program status and generating the reports. A standard report contains the list of devices and notifications about the following events:

- **A change in the set of devices**. A device has not been detected.
- **A critical change in the set of devices**. Two devices have not been detected.
- **System loading with the password**.
- **Main system functions are performed**: disk/partition is encrypted or decrypted, the boot loader is installed or removed, the password is changed, or the set of devices is modified.

The standard log file is available at

```
C:\Windows\DecryptLog.log
```

Detailed information about the encryption system events and the reasons of operation failures is provided in the detailed event log available at

```
C:\ProgramData\DeCrypt\DeCrypt.log
```

For both types of reports, SoftControl DeCrypt supports log rotation, which allows managing the size of the log files. Rotation allows the logs to be automatically divided into parts of the following type (all parts have identical parameters):

- *DeCryptLog(rotated dd.mm.yyyy).log* for standard log files, where dd.mm.yyyy is the date of the log rotation;
- *DeCrypt.log_old1*, *DeCrypt.log_old2*, etc. for detailed log files.

The log file is rotated after its size exceeds 100MB.

Note. Duplicated USB drives are only specified in the `DecryptLog.log` standard log file once. However, if two USB drives have the same VID and PID parameters, and one of the drives has a serial number while the other does not have it, then both devices are specified in the log file (the entries are duplicated).

4.8 Black list of devices and delayed start

If the client host has devices that take a lot of time to initialize, there are two ways to improve the client host's performance:

A. Delay the boot loader start (specify a delay during OS loading). Total time required to load the client host increases in this case.

B. Exclude the devices from the list of devices to be checked, i.e. blacklist the devices. In this case, the loading time decreases; however, the blacklisted devices are not used to decrypt the disk.

To add USB drive to the black list, perform the following operations:

1) Find the identifier of the device you do not want to check, in the `DeCryptLog.log` log file (the path is `C:\Windows\DeCryptLog.log`). USB drives are listed in the log file as `VID_PID_SERIALNUMBER`.
   Important: The entry is only available in the log in the device has been detected during client host loading.

2) Run Windows Command Prompt with the administrator privileges. Mount the EFI partition to the disk with the help of the following command:

```
mountvol u: /s
```

   where u: is the name of the disk to mount to.

3) Open the settings file in Notepad with the following command:

```
notepad.exe u:\EFI\DeCrypt\DcsProp
```

4) Change the string

```
<config key="BlacklistDevices"></config>
```

   to

```
<config key="BlacklistDevices">device1;device2;...;deviceN</config>
```

   where `deviceN` is the full device identifier (as specified in the log file), or the beginning of the identifier and the * mask (Latin letters, figures and underline).

   Example:

```
<config key="BlacklistDevices">13FE_4200_P16019100703681B1EDD8A13;0E0F_*</config>
```

5) Update the list of devices with the following command:

```
"<SoftControl DeCrypt installation folder>\DcConsole.exe" /dev-change /currpassfile
```

```
<file with current password>
```

To specify a delay during OS loading, perform the following operations:

1) Open the settings file with the following command:

```
notepad.exe u:\EFI\DeCrypt\DcsProp
```

2) Set the required delay value (in seconds) for the `UsbInitDelay` parameter.

4.9 Generating encrypted data

The *DcUtil.exe* utility is designed to generate encrypted data blocks. When you implement automatic SoftControl DeCrypt control with the help of third-party software, you can use the utility to enable safe password transfer.

The utility is part of the SoftControl DeCrypt installation package; however, it is not installed when you install SoftControl DeCrypt. To work with it, you need to copy it to the control computer manually.

The procedure is described below.

1) From the control computer, run the following command on the computer with the installed SoftControl DeCrypt.

   ```
   "<SoftControl DeCrypt installation folder>\DcConsole.exe" /seed-get
   ```

   The result is a one-time encrypted data block of the following form.

   ```
   242d3695c45b5...9fch
   ```

2) Copy the data block to the control computer.

3) Run the following command on the control computer.

   ```
   "<folder with DcUtil.exe>\DcUtil.exe" /<command> [<parameters>]
   ```

   The result is a one-time encrypted data block (`seed_value`) of the following form.

   ```
   bb4e05cdc6c6bca94506b4dce81fd7791fa9cdff0...4258527h
   ```

4) From the control computer, run the required command (see table above [24]) on the computer with the installed SoftControl DeCrypt. Use the encrypted data block obtained in step 3) as a password.

Table 7 lists available commands for *DcUtil.exe* and their parameters.

Important: all steps require administrator privileges.

Table 7. DcUtil.exe command line parameters

Command/Parameter	Action/Possible values
`/help`	Display the list of commands
`/encryptpasswords [/currpass` *`current_password`*`] [/newpass` *`new_password`*`] (/seed` *`seed_value`*`|` `/seedfile` *`file_with_seed_value`*`)`	Encrypt current password, new password, or both. The values are as follows. a) *current_password*; see above 24 for details on how to set the password; b) *new_password*; see above 24 for details on how to set the password; c) *seed_value* or *file_with_seed_value* generated by *DcConsole.exe* (see above 28).

5. Updating SoftControl DeCrypt

This section describes operations that are required to updated SoftControl DeCrypt:

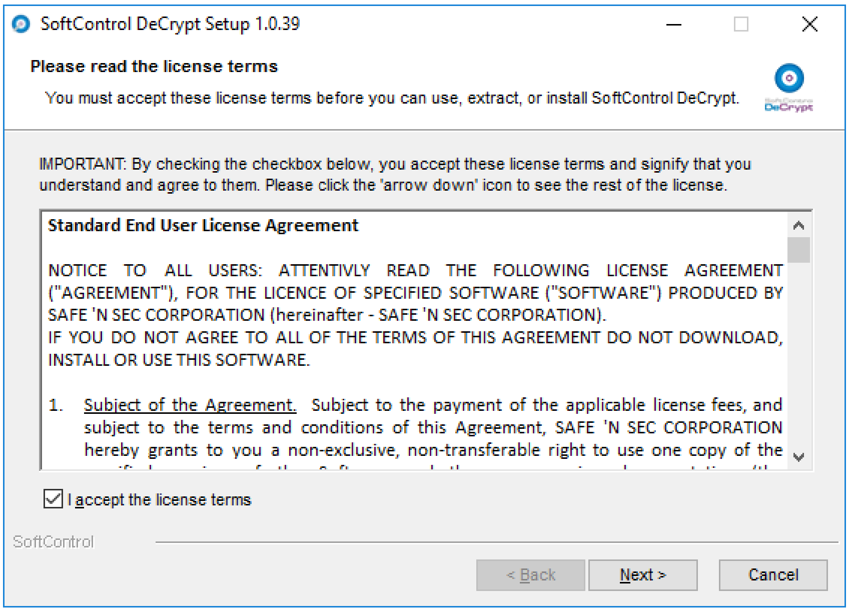
- in standard mode 30;
- in silent mode 33.

You can update SoftControl DeCrypt without decrypting the disk.

5.1 Updating in standard mode

1) Run the *SoftControl DeCrypt Setup <product version>* installation package of the version you want to update to.

2) If you accept the terms, select **I accept the license terms** and click **Next** (fig. License agreement 30).



SoftControl DeCrypt Setup 1.0.39

Please read the license terms

You must accept these license terms before you can use, extract, or install SoftControl DeCrypt.

IMPORTANT: By checking the checkbox below, you accept these license terms and signify that you understand and agree to them. Please click the 'arrow down' icon to see the rest of the license.

Standard End User License Agreement

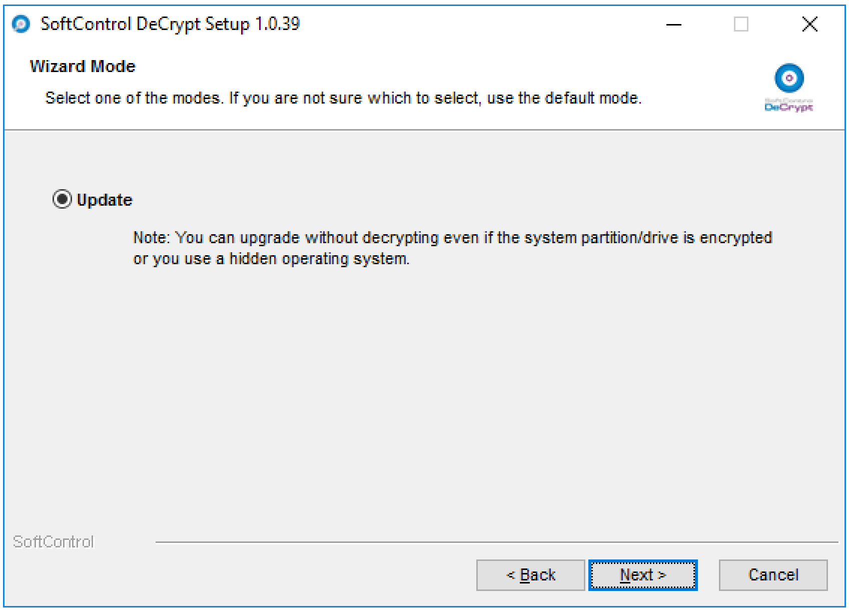
NOTICE TO ALL USERS: ATTENTIVLY READ THE FOLLOWING LICENSE AGREEMENT ("AGREEMENT"), FOR THE LICENCE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY SAFE 'N SEC CORPORATION (hereinafter - SAFE 'N SEC CORPORATION).
IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

1. Subject of the Agreement. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, SAFE 'N SEC CORPORATION hereby grants to you a non-exclusive, non-transferable right to use one copy of the

☑ I accept the license terms

Figure 31. License agreement

3) Select the required option in the **Wizard Mode** window and click **Next** (fig. Selecting the update option 30).



SoftControl DeCrypt Setup 1.0.39

Wizard Mode

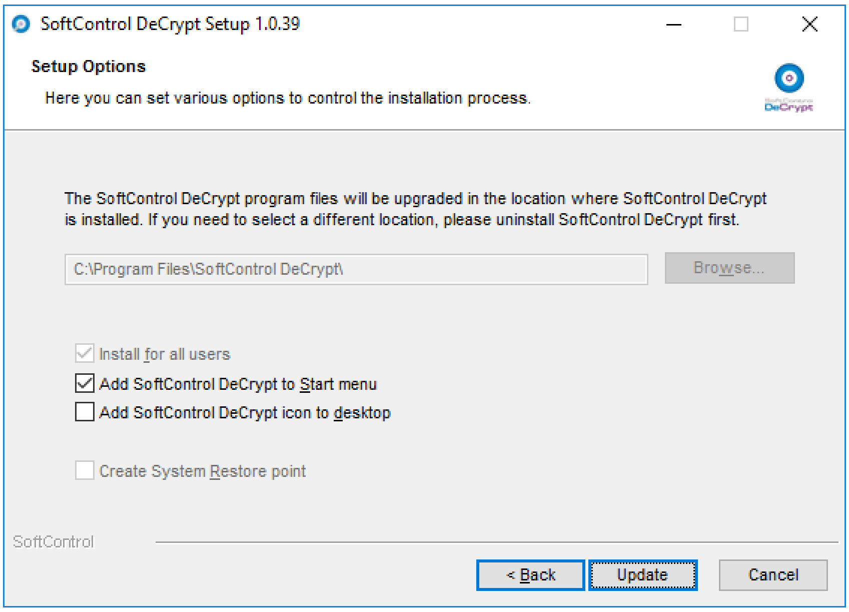
Select one of the modes. If you are not sure which to select, use the default mode.

● **Update**

Note: You can upgrade without decrypting even if the system partition/drive is encrypted or you use a hidden operating system.

Figure 32. Selecting the update option

4) Select the required options in the **Setup options** window and click **Update** (fig. Selecting setup options [31]).



SoftControl DeCrypt Setup 1.0.39

Setup Options

Here you can set various options to control the installation process.

The SoftControl DeCrypt program files will be upgraded in the location where SoftControl DeCrypt is installed. If you need to select a different location, please uninstall SoftControl DeCrypt first.

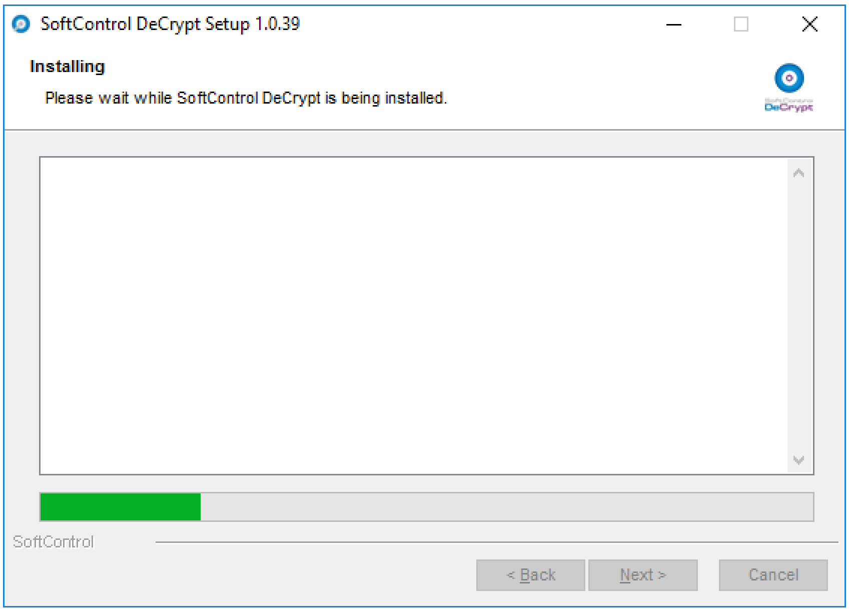
C:\Program Files\SoftControl DeCrypt\

☑ Install for all users
☑ Add SoftControl DeCrypt to Start menu
☐ Add SoftControl DeCrypt icon to desktop

☐ Create System Restore point

Figure 33. Selecting setup options

5) Wait until the update completes (fig. Update progress [31]).



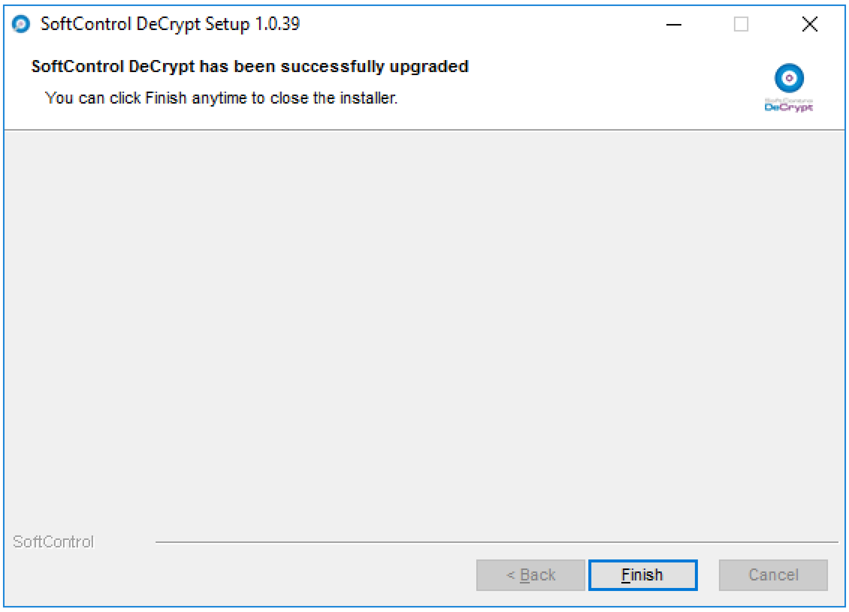
SoftControl DeCrypt Setup 1.0.39

Installing

Please wait while SoftControl DeCrypt is being installed.

Figure 34. Update progress

6) After the **SoftControl DeCrypt has been successfully upgraded** message is displayed, click **Finish** (fig. Update completes[32]).



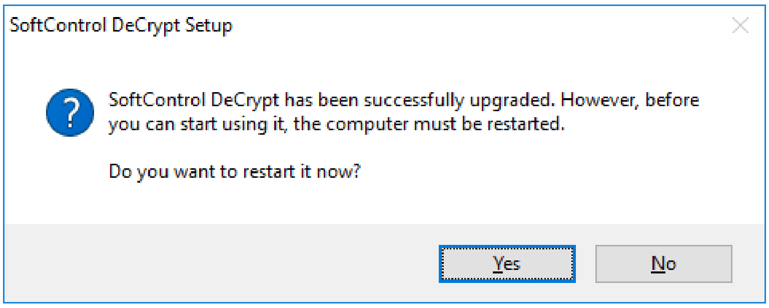
SoftControl DeCrypt Setup 1.0.39

SoftControl DeCrypt has been successfully upgraded

You can click Finish anytime to close the installer.

Figure 35. Update completes

7) Select **Yes** in the dialog box that suggests system reboot. The system is then restarted to complete the updates (fig. Requesting system reboot[32]).



SoftControl DeCrypt Setup

SoftControl DeCrypt has been successfully upgraded. However, before you can start using it, the computer must be restarted.

Do you want to restart it now?

Figure 36. Requesting system reboot

5.2 Updating in silent mode

Important: all steps require administrator privileges.

1) Copy the *SoftControl DeCrypt Setup <product version>.exe* installation package of the version you want to update to, to a directory on the client host.

2) Run Windows command prompt and enter the following command:

```
"<folder with the installation package>\SoftControl DeCrypt Setup <product version>.exe" /q
```

6. Removing SoftControl DeCrypt

This section describes how to uninstall SoftControl DeCrypt:

- in standard mode (via GUI) 34;
- in silent mode 35.

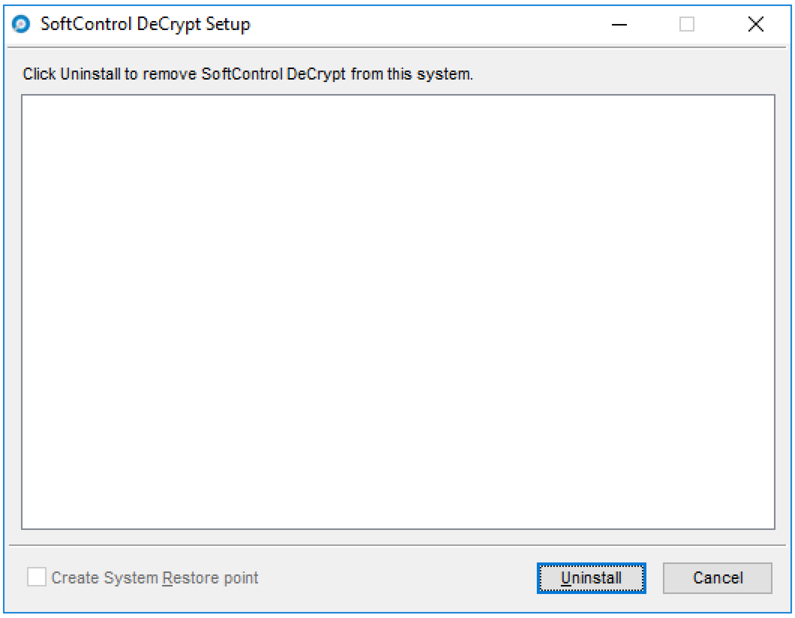
You need to decrypt the disk before you uninstall SoftControl DeCrypt.

6.1 Removing in standard mode

1) For Microsoft® Windows® Server 2003: go to Windows Control Panel → **Add or Remove Programs** → **Change or Remove Programs**, select *SoftControl DeCrypt* and click **Remove**.

For Microsoft® Windows® 7, Microsoft® Windows® Server 2008, Microsoft® Windows® 8, Microsoft® Windows® Server 2012, Microsoft® Windows® 10, Microsoft® Windows® Server 2016: go to Windows Control Panel → **Programs** → **Uninstall program**, select *SoftControl DeCrypt* and click **Uninstall**.

1) In the displayed window, click **Remove** (fig. Confirming deinstallation 34).

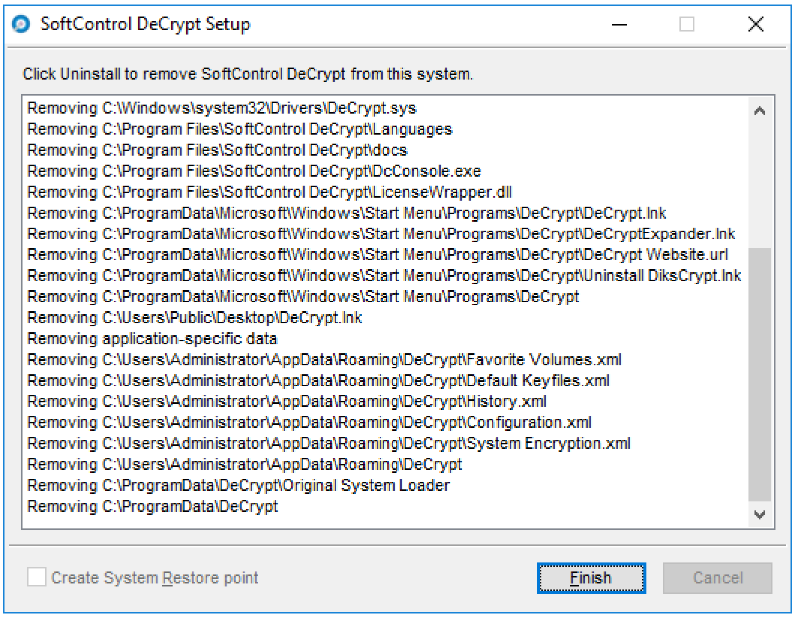

SoftControl DeCrypt Setup

Click Uninstall to remove SoftControl DeCrypt from this system.

Figure 37. Confirming deinstallation

Note. If you added any files to the SoftControl DeCrypt installation folder, the installation wizard does not remove the folder.

Click **Finish** to complete the process (fig. Deinstallation completes 34).



Click Uninstall to remove SoftControl DeCrypt from this system.

```
Removing C:\Windows\system32\Drivers\DeCrypt.sys
Removing C:\Program Files\SoftControl DeCrypt\Languages
Removing C:\Program Files\SoftControl DeCrypt\docs
Removing C:\Program Files\SoftControl DeCrypt\DcConsole.exe
Removing C:\Program Files\SoftControl DeCrypt\LicenseWrapper.dll
Removing C:\ProgramData\Microsoft\Windows\Start Menu\Programs\DeCrypt\DeCrypt.lnk
Removing C:\ProgramData\Microsoft\Windows\Start Menu\Programs\DeCrypt\DeCryptExpander.lnk
Removing C:\ProgramData\Microsoft\Windows\Start Menu\Programs\DeCrypt\DeCrypt Website.url
Removing C:\ProgramData\Microsoft\Windows\Start Menu\Programs\DeCrypt\Uninstall DiksCrypt.lnk
Removing C:\ProgramData\Microsoft\Windows\Start Menu\Programs\DeCrypt
Removing C:\Users\Public\Desktop\DeCrypt.lnk
Removing application-specific data
Removing C:\Users\Administrator\AppData\Roaming\DeCrypt\Favorite Volumes.xml
Removing C:\Users\Administrator\AppData\Roaming\DeCrypt\Default Keyfiles.xml
Removing C:\Users\Administrator\AppData\Roaming\DeCrypt\History.xml
Removing C:\Users\Administrator\AppData\Roaming\DeCrypt\Configuration.xml
Removing C:\Users\Administrator\AppData\Roaming\DeCrypt\System Encryption.xml
Removing C:\Users\Administrator\AppData\Roaming\DeCrypt
Removing C:\ProgramData\DeCrypt\Original System Loader
Removing C:\ProgramData\DeCrypt
```

☐ Create System Restore point

Figure 38. Deinstallation completes

6.2 Removing in silent mode

Important: all steps require administrator privileges.

Run Windows command prompt and enter the following command:

```
"<SoftControl DeCrypt installation folder>\SoftControl DeCrypt Setup.exe" /q /u
```

7. Customer support

If you have any questions concerning the installation, setting up and operation of SoftControl DeCrypt, please contact our customer support by e-mail support@safensoft.com.

8. Appendix

8.1 Setting up the disk partition

This section contains general information on how to prepare the first volume of the system disk to install SoftControl DeCrypt. The information provided is a recommendation only and can be used if errors occur during SoftControl DeCrypt installation.

If the SoftControl DeCrypt installer displays an error that there is not enough space on the disk, you can perform the following operations.

Important: all steps require administrator privileges.

Usually, the first volume on the disk is reserved by Windows for system recovery and is not used during normal system operation. You can delete this volume. To do so, run Windows Command Prompt with the following command:

```
compmgmt.msc
```

In the displayed **Computer management** snap-in, select **Disk management**. Right-click the first volume and select **Delete volume...**. Follow the instructions in the displayed window to remove the volume.

You can only perform this operation if you are sure the first volume does not contain important data.

If you need to retain the information, use one of the disk management software to decrease the volume and move it away from the beginning of the disk, so that free space becomes available for SoftControl DeCrypt installation.

Note. If the first volume is not visible in the **Computer management** snap-in in your OS, you can use the `diskpart.exe` command line utility.