SoftControl

DeCrypt 6.0.187

Administrator guide

Dear user!

ARUDIT SECURITY, LLC 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.

Postal address:

127106 Russia, Moscow

Botanicheskaya street, house number 10d building 1

ARUDIT SECURITY, LLC

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

Contents

1. Introduction

1.1 Purpose

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

1. The violator steals the hard disk of a computer. The violator reverse engineers the contents of the disk in a lab, finds software vulnerabilities and subsequently carries out an attack on the computer.
2. The violator bypasses BIOS protection, loads the computer 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 runs 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. It is acceptable to change fewer devices*[4].

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'.

* Creating a key from a subset of devices is cryptographically strong due to the use of the Shamir's secret sharing algorithm.

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
	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 the page numbers, or links to external resources (URL).

1.2.2 List of acronyms

This documents uses the following acronyms:

- **CPU** – central processing unit;
- **HDD** – hard disk drive;
- **OS** – operating system;
- **RAM** – random access memory;
- **SSD** – self-service device.

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.

Term	Description
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	CPU frequency	RAM size	HDD free space
Client operating systems:			100MB + extra 10MB in the UEFI partition
Microsoft® Windows® 7 (SP1) *64-bit*[1]	1GHz	2GB	
Microsoft® Windows® 8 *32-bit*	1GHz	1GB	
Microsoft® Windows® 8 *64-bit*	1GHz	2GB	
Microsoft® Windows® 8.1 *32-bit*	1GHz	1GB	
Microsoft® Windows® 8.1 *64-bit*	1GHz	2GB	
Microsoft® Windows® 10 *32-bit*	1GHz	1GB	
Microsoft® Windows® 10 *64-bit*	1GHz	2GB	
Microsoft® Windows® 10 IoT Enterprise *32-bit*	1GHz	1GB	
Microsoft® Windows® 10 IoT Enterprise *64-bit*	1GHz	2GB	
Server operating systems:			
Microsoft® Windows® Server 2008 R2 *64-bit*[1,2]	1.4GHz	512MB	
Microsoft® Windows® Server 2012 *64-bit*[2]	1.4GHz	512MB	
Microsoft® Windows® Server 2012 R2 *64-bit*[2]	1.4GHz	512MB	
Microsoft® Windows® Server 2016 *64-bit*[2]	1.4GHz	512MB	

Примечания:

1. Update KB3033929 or equivalent (support of the SHA-256 algorithm for digital signature verification).
2. Only desktop installation options are supported.

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 38.

3. Installing SoftControl DeCrypt

You can install SoftControl DeCrypt in the following ways:

- standard mode (via GUI) [8];
- silent mode [10].

3.1 Installing in standard mode

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

2) If you accept the terms, select **I accept the license** and click **Next** (fig. License agreement [8]).

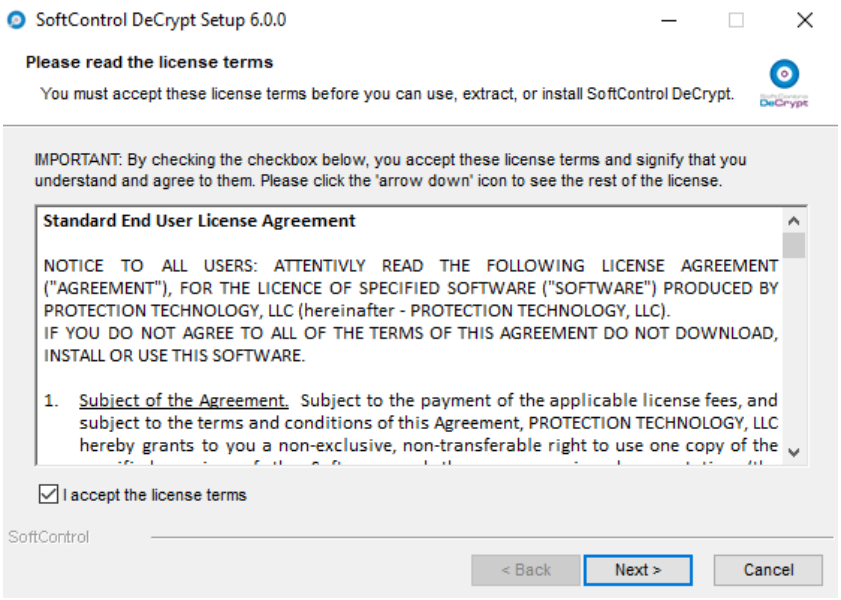

Figure 1. License agreement

3) Select the required option in the **Wizard Mode** window and click **Next** (fig. Selecting the installation option [9]).

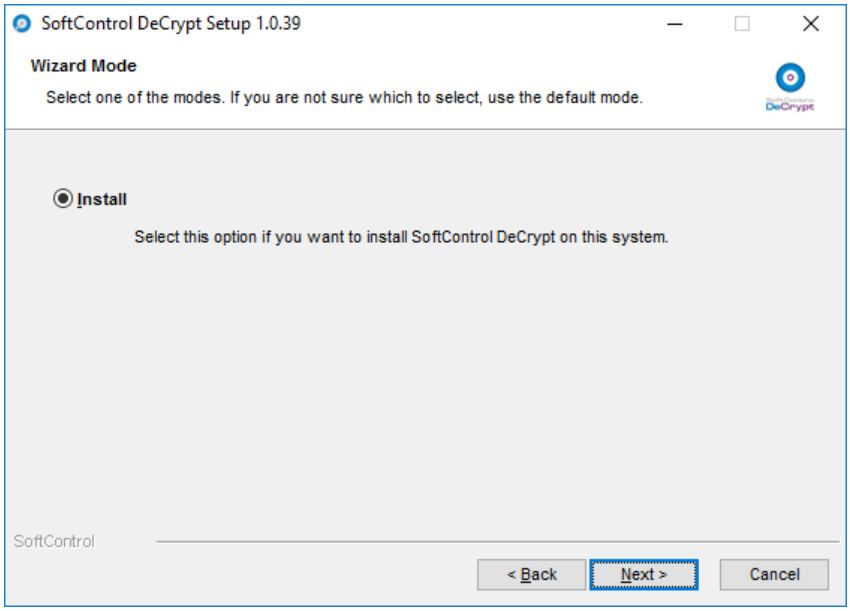

Figure 2. Selecting the installation option

4) Select a directory to install SoftControl DeCrypt to (with the help of the **Browse** button) and click **Next** (fig. Installation path 9).

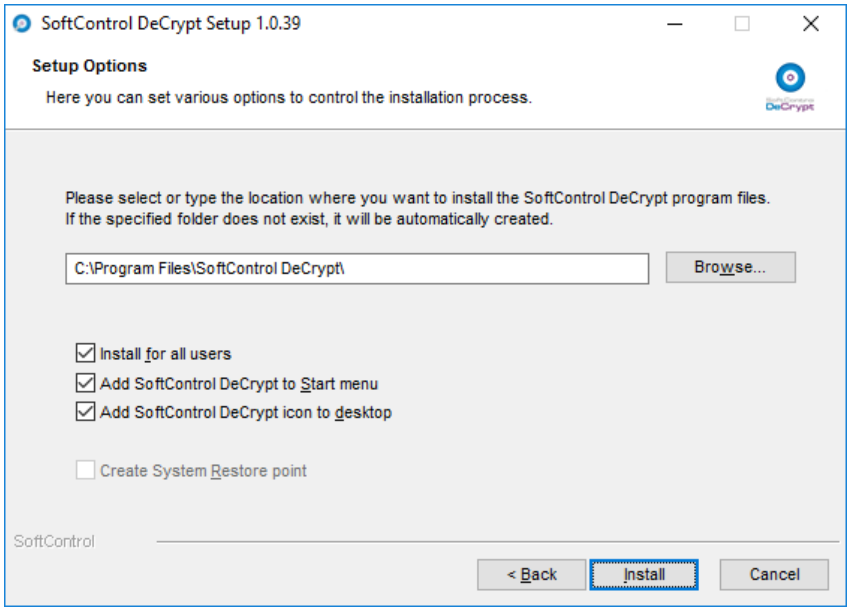

Figure 3. Installation path

5) Wait until installation completes (fig. Installation progress 10).

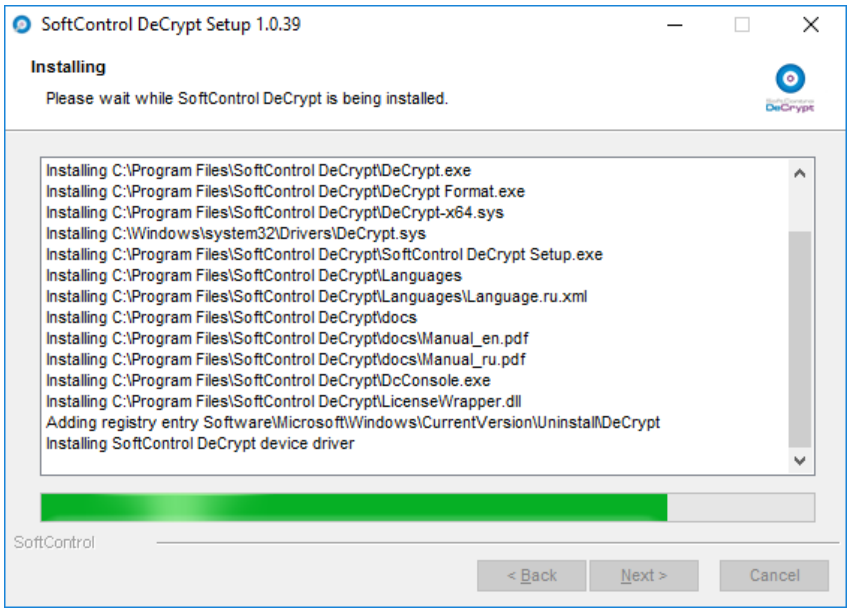

Figure 4. Installation progress

6) After the **SoftControl DeCrypt has been successfully installed** message is displayed, click **Finish** (fig. Installation completes [10]).

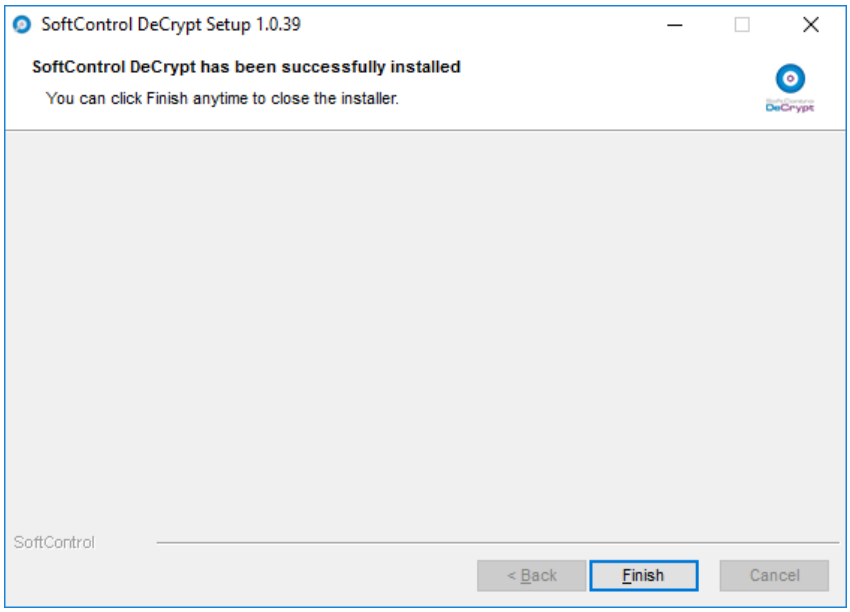

Figure 5. Installation completes

3.2 Installing in silent mode

Important: All steps require administrator privileges.

1) Copy the *SoftControl DeCrypt Setup.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.exe" /q [/folder "<install-
ation 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.

Important: All operations require administrator privileges.

SoftControl DeCrypt GUI is shown in fig. Elements of the program GUI 12.

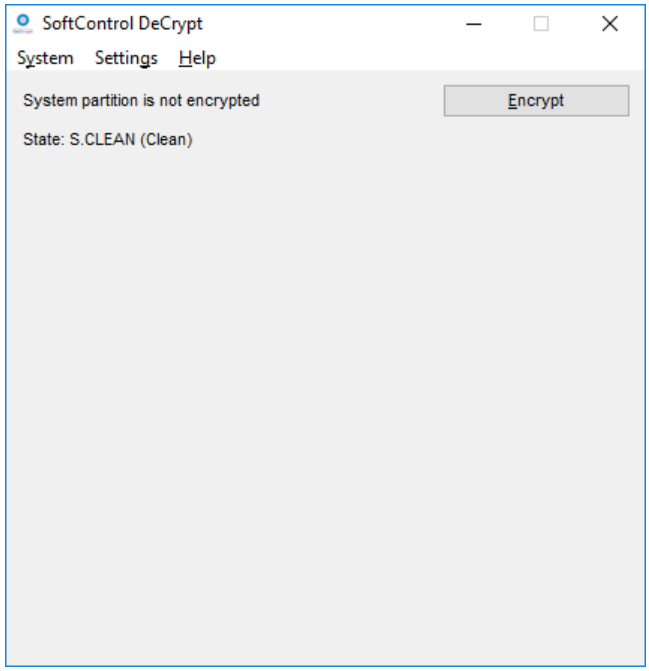

Figure 6. Elements of the program GUI

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 re-booted).
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 12).

In the displayed window, select **Encryption algorithm** and **Hash algorithm** from the drop-down lists and click **Next** (fig. Encryption options 13). Hash algorithm is used to generate keys from the password and other data, as well as to generate random numbers.

Figure 7. Encryption options

Set the **Password** and confirm it (fig. Specifying the password 14).

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 14).

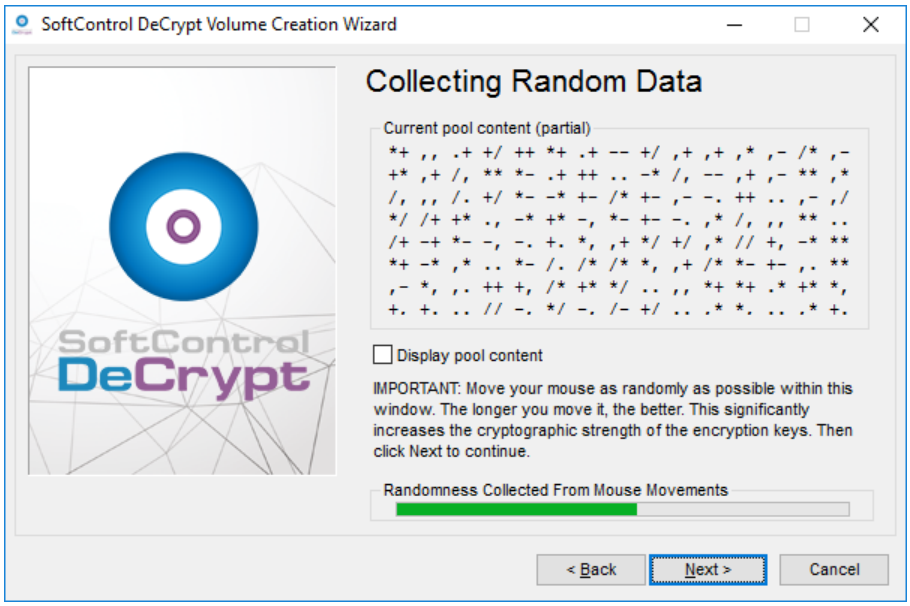

Figure 9. Collecting random data

To view the keys in the next window (fig. Generated keys 15), tick off **Display generated keys (their portions)**.

Figure 10. Generated keys

Select the **Wipe mode** from the drop-down list (fig. Selecting wipe mode 15).

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 15), 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 16).

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 16).

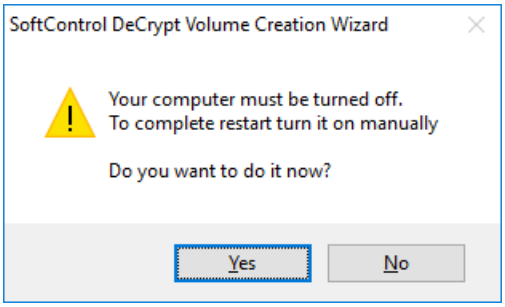

Figure 13. Turning off the computer

After the client host boots, SoftControl DeCrypt displays a message about resuming disk encryption 16 (provided that the user logs in with the account he/she used to start the encryption process); then a message that the pretest has completed (fig. Pretest completed 17).

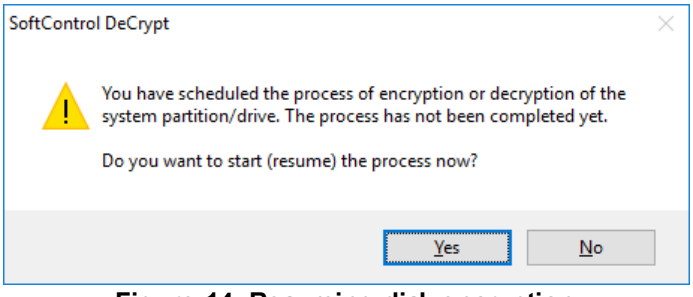

Figure 14. Resuming disk encryption

Figure 15. Pretest completed

Click **Encrypt** to run disk encryption. The **Encryption** window displays the progress bar and the remaining time (fig. Disk encryption 17).

Figure 16. 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 12).

You cannot cancel the encryption process.

Note. The message about resuming disk encryption (see figure above[16]) is also displayed after encryption is interrupted and the client host restarts, provided that the user logs in with the account he/she used to run the encryption process.

After the encryption process completes, click **OK** in the displayed window (fig. Encryption completed[18]); then click **Finish** in the Volume creation wizard window (fig. Disk is encrypted[18]).

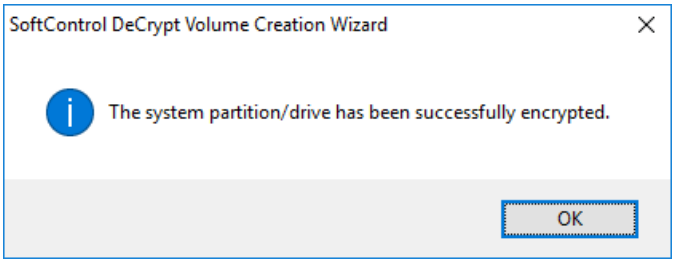

Figure 17. Encryption completed

Figure 18. Disk is encrypted

When you run SoftControl DeCrypt next time, the main window displays the encryption parameters (fig. Encryption parameters[19]).

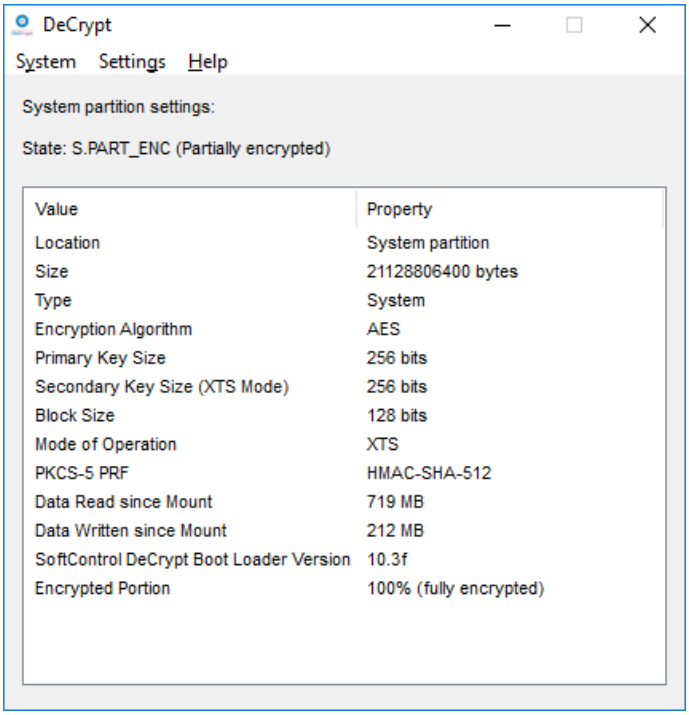

Figure 19. Encryption parameters

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 20).

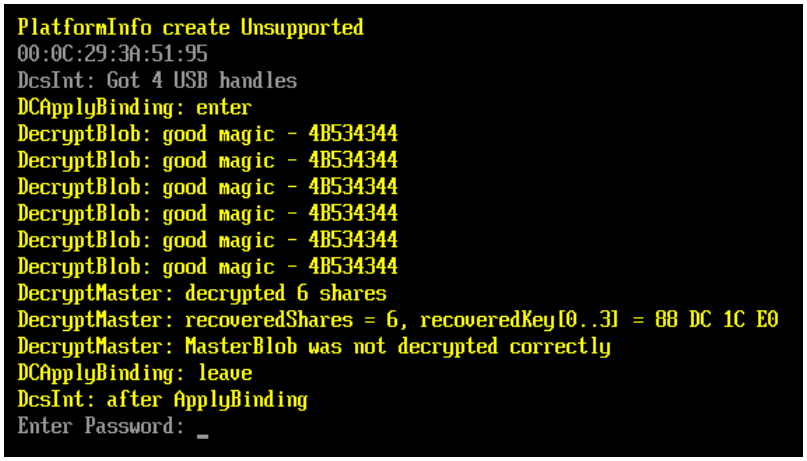

Figure 20. Requesting the password when loading the client host

When you run disk encryption, SoftControl DeCrypt reads out the parameters of the devices detected during the 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 12). Select **Yes** in the message with the warning (fig. Confirming disk decryption 20) and wait till the process completes (fig. The disk is decrypted 21).

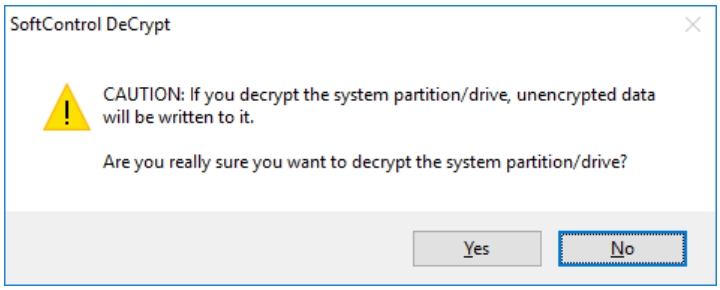

Figure 21. Confirming disk decryption

As with the encryption (see section Encrypting system volume 17), you can interrupt or postpone the process by clicking **Pause** or **Defer** (fig. Decrypting the disk 21).

Figure 22. Decrypting the disk

You cannot cancel the decryption process.

Note. If decryption has been interrupted, SoftControl DeCrypt displays the following message after the client host boots next time (fig. Resuming disk decryption 21), provided that the user logs in with the account he/she used to run the decryption process.

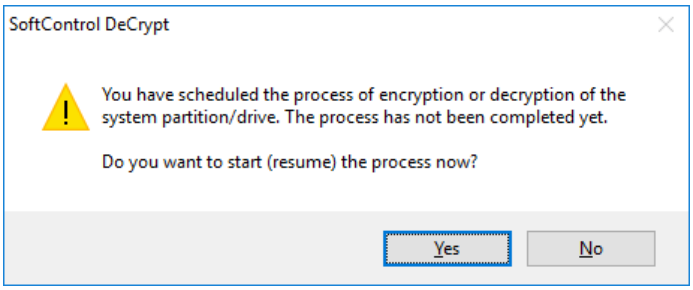

Рисунок 23. Resuming disk decryption

Click **OK** in the displayed window (fig. The disk is decrypted 21).

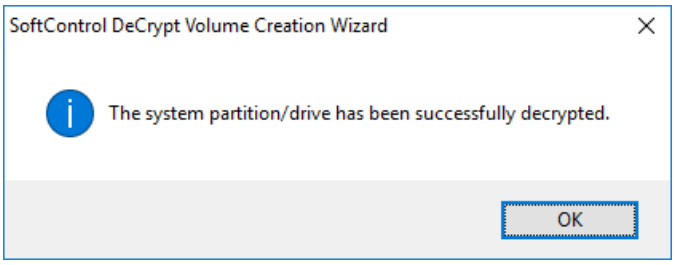

Figure 24. The disk is decrypted

Click **Yes** In the dialog box that suggests system reboot. The client host then reboots to complete the process (fig. Requesting system reboot 22).

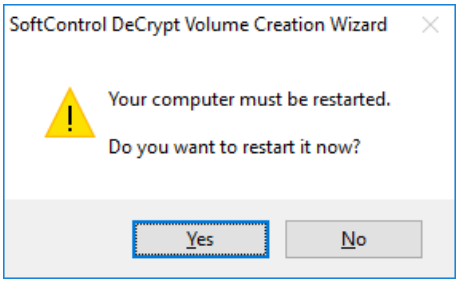

Figure 25. Requesting system reboot

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 22).

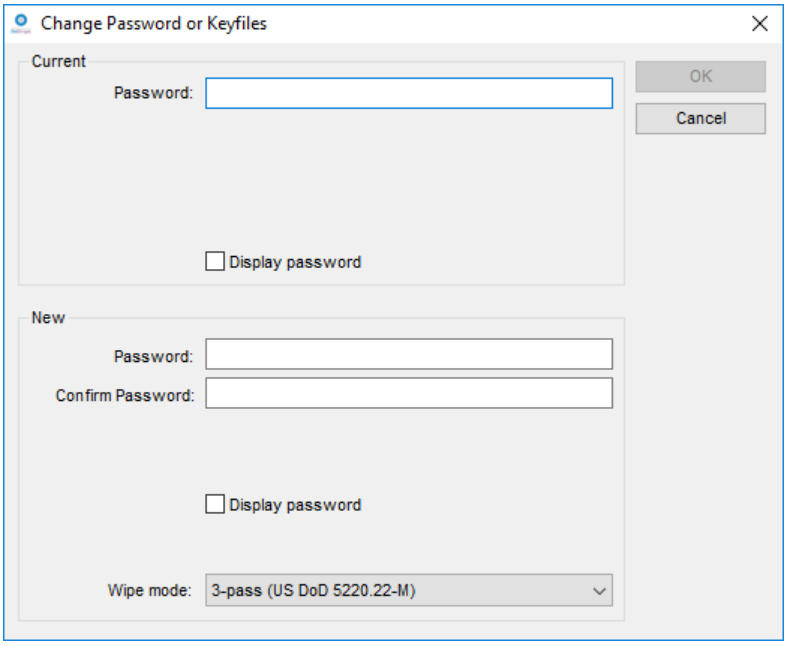

Figure 26. Changing the password

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 23), just as you did to generate keys for encryption (see fig. Collecting random data 14).

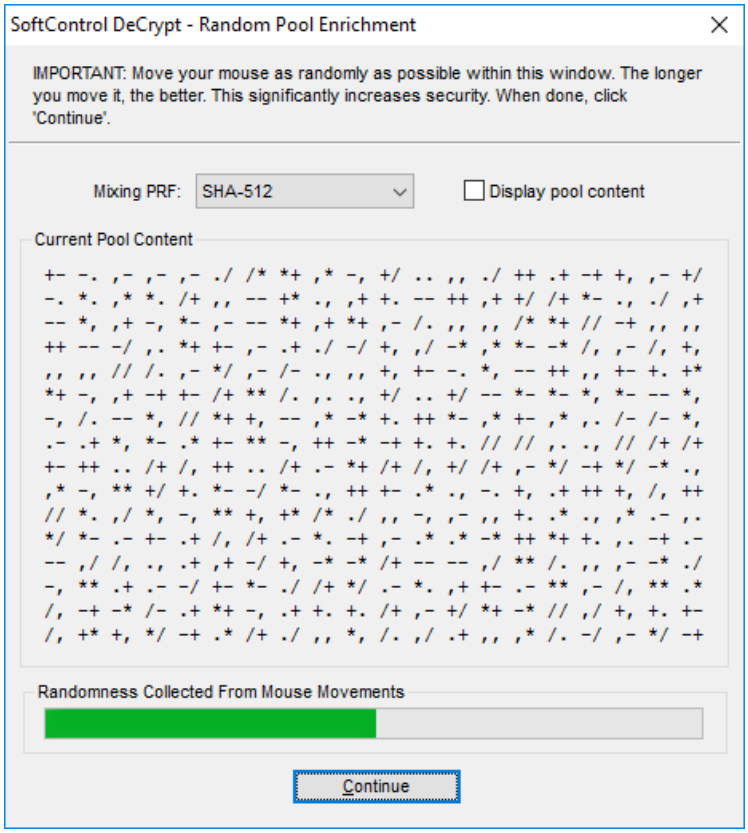

Figure 27. Collecting random data to change the password

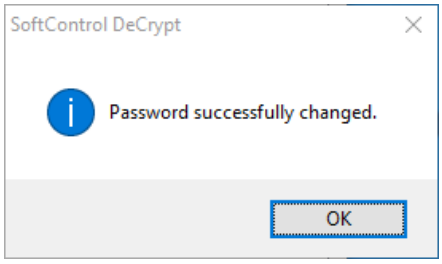

Figure 28. Password has been changed

To complete the process, click **Continue** (see above 23) and **OK** (fig. Password has been changed 23).

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 24).

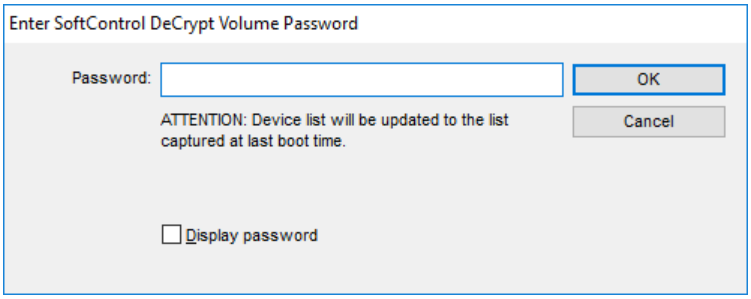

Figure 29. Entering the password to change the connected devices

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 24).

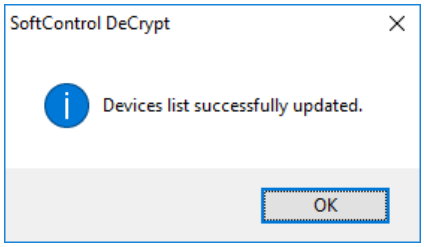

Figure 30. The list of devices is updated

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 [29]), with the help of the /cryptpass parameter. d) specify *file_with_encrypted_data_block* (generated by DcUtil.exe [29]), 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.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 Logs

SoftControl DeCrypt enables logging the events and the program status. A standard log file 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 or 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 files, 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 List of ignored 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. In this case, the loading time decreases; however, the ignored devices are not used to decrypt the disk.

To add USB drive to the ignore 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[25]) 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

Command/Parameter	Action/Possible values
/encryptpasswords [/currpass *current_password*] [/newpass *new_password*] (/seed *seed_value*| /seedfile *file_with_seed_value*)	Encrypt current password, new password, or both. You can specify the password in the following ways. a) specify the *current_password* and the *new_password* explicitly. See above [25] for details on how to set the password. b) specify the *seed_value* generated by *DcConsole.exe* (see above [29]), with the help of the /seed parameter. c) specify the *file_with_seed_value* generated by *DcConsole.exe*, with the help of the /seedfile parameter.

4.10 License expiration

After SoftControl DeCrypt license expires, the following functions become unavailable.

- Installing the boot loader.
- Encrypting disk or partition.
- Creating a new list of devices that are used for system loading.
- Changing the password that is used to load the system if there is a critical change in the set of devices.

If you try to run one of these functions, SoftControl DeCrypt displays license expiration message and prompts you to enter a license key.

Other SoftControl DeCrypt functions (decrypting the disk, removing the boot loader, etc.) are still available in this case.

5. Updating SoftControl DeCrypt

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

- in standard mode [31];
- in silent mode [34].

> 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 [31]).

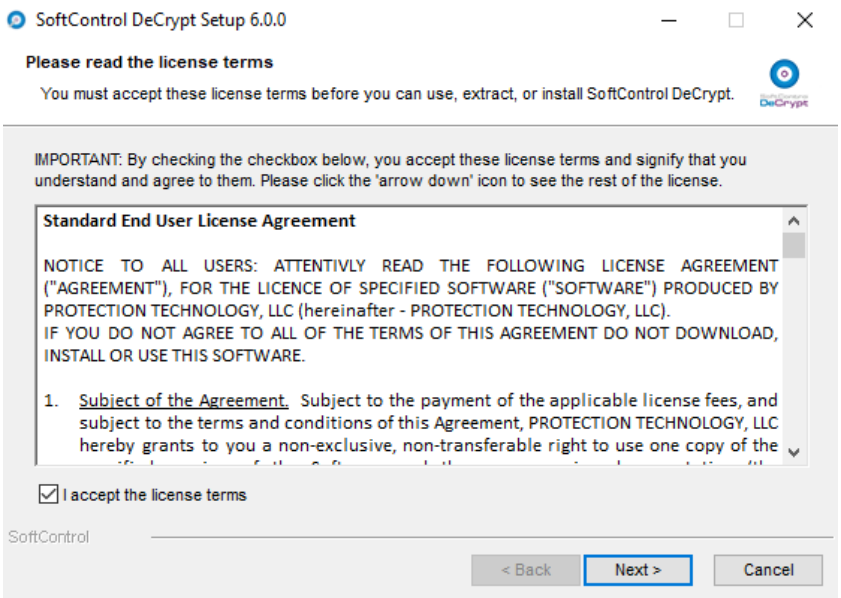

Figure 31. License agreement

3) Select the required option in the **Wizard Mode** window and click **Next** (fig. Selecting the update option [32]).

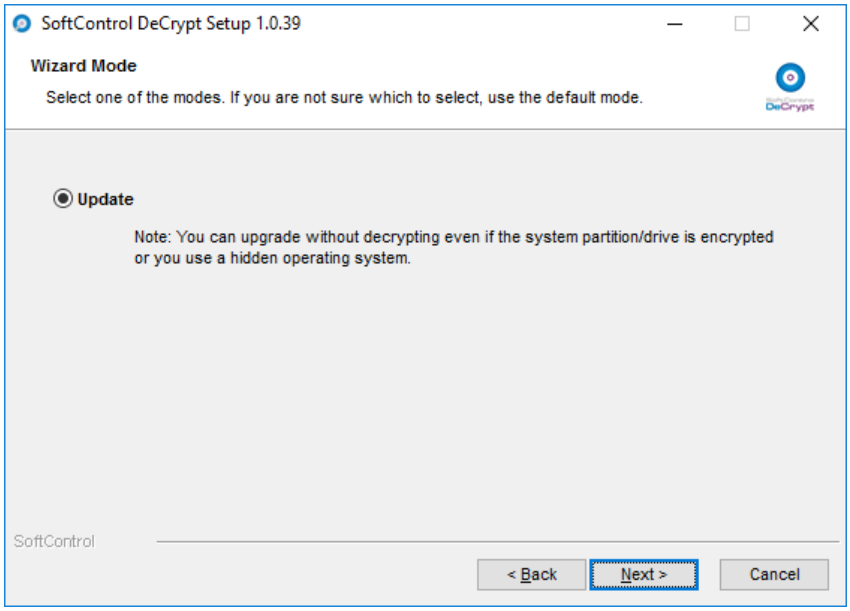

Figure 32. Selecting the update option

4) Select the required options in the **Setup options** window and click **Update** (fig. Selecting setup options 32).

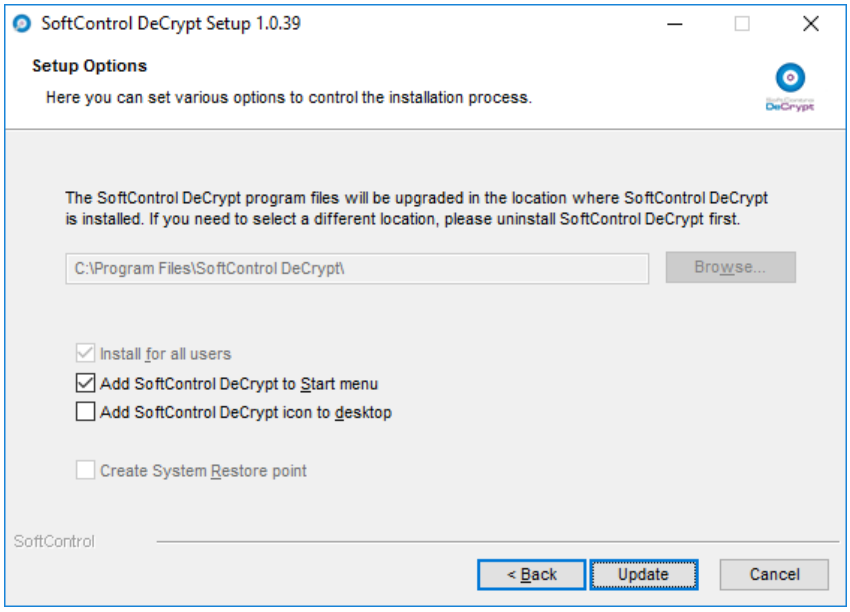

Figure 33. Selecting setup options

5) Wait until the update completes (fig. Update progress 33).

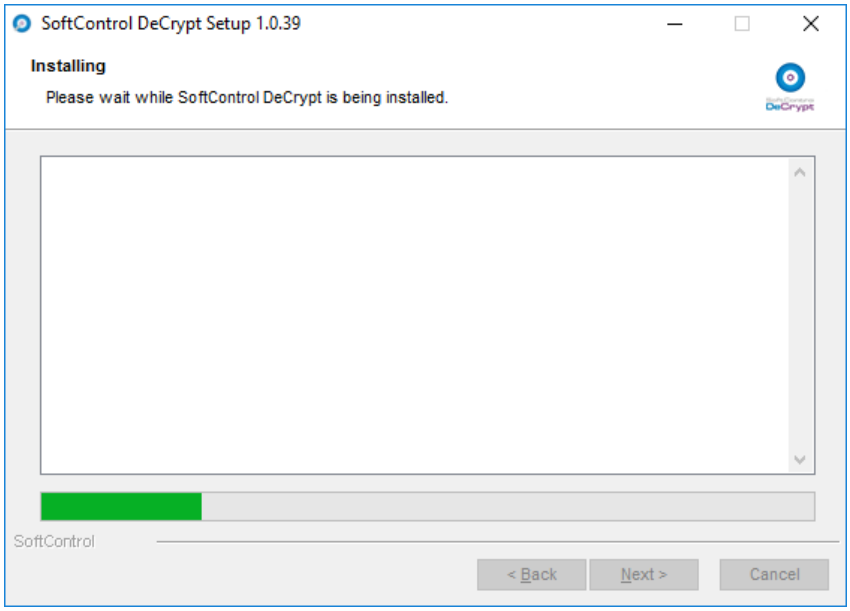

Figure 34. Update progress

6) After the **SoftControl DeCrypt has been successfully upgraded** message is displayed, click **Finish** (fig. Update completes 33).

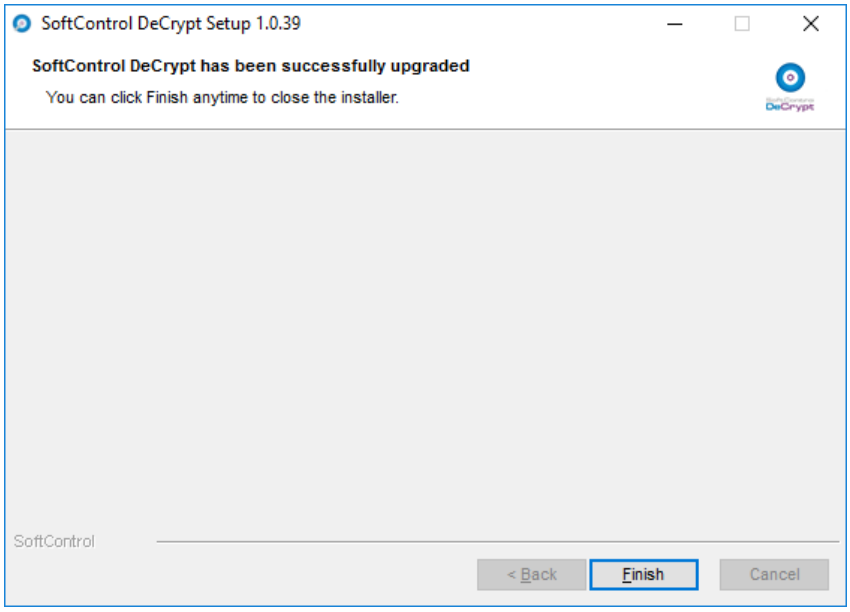

Figure 35. Update completes

7) Select **Yes** in the dialog box that suggests system reboot. The system is then restarted to complete the updates (fig. Requesting system reboot 34).

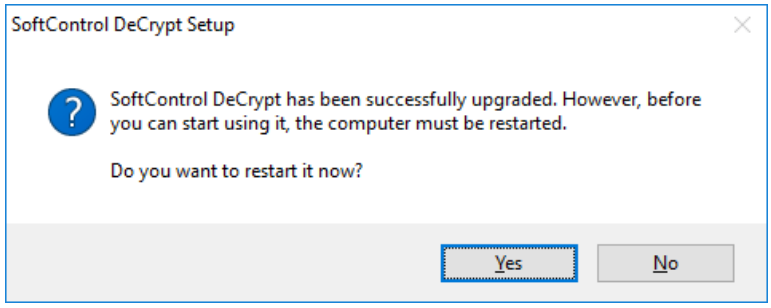

Figure 36. Requesting system reboot

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
```

To ensure proper functioning of the SoftControl DeCrypt component, manually restart the device after updating in silent mode. It is necessary for updating of the driver.

6. Removing SoftControl DeCrypt

This section describes how to uninstall SoftControl DeCrypt:

- in standard mode (via GUI) 35;
- in silent mode 36.

You need to decrypt 20 system volume before you uninstall SoftControl DeCrypt. Otherwise, you will not be able to restore its contents.

6.1 Removing in standard mode

1) 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**.
2) In the displayed window, click **Remove** (fig. Confirming deinstallation 35).

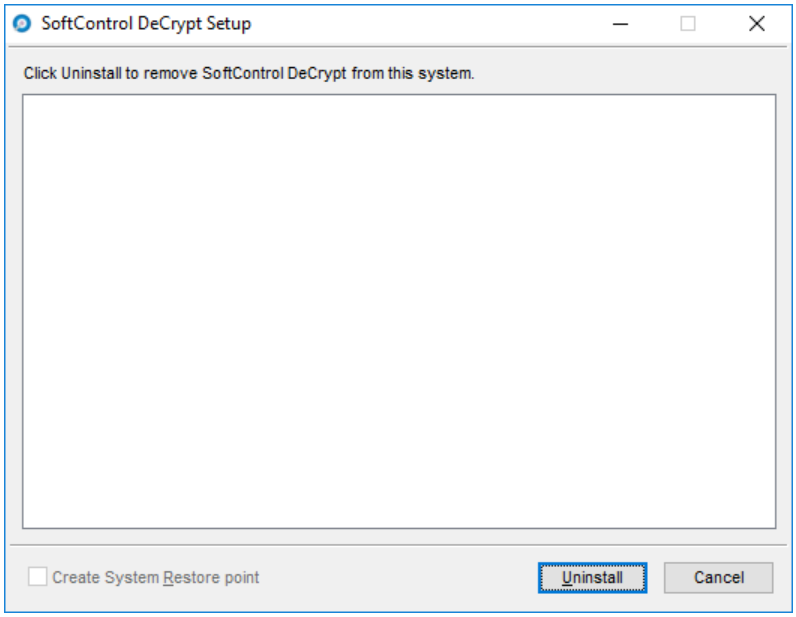

Figure 37. Confirming deinstallation

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 36).

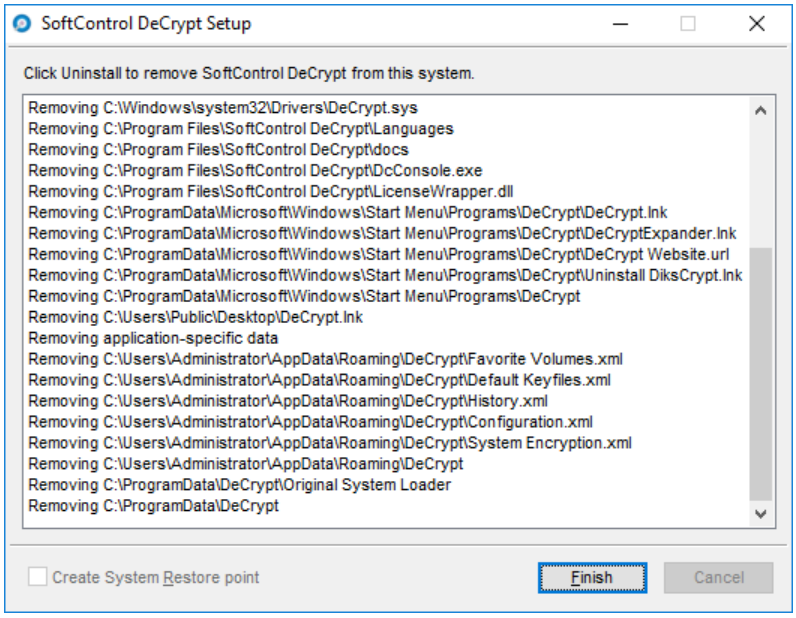

Figure 38. Deinstallation completes

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 and if you are not going to restore the OS from the system disk should the OS malfunction. If you need to restore the OS after you remove the first volume, you can do so by loading the OS from a USB drive or an optical disc.

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. Below are the examples of software:

- GParted (live-cd);
- Acronis Disk Director;
- Paragon Partition Manager;
- EaseUS Partition Master;
- Windows Image Backup;
- Clonezilla;
- GParted;
- Acronis True Image;

- HDClone.

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.