Kaspersky Lab AO
39A/2 Leningradskoe Shosse,
Moscow, 125212, Russia

T. +7 495 797 87 00
www.kaspersky.com
www.securelist.com

Preparative Procedures for Kaspersky Endpoint Security for Windows

Document version 1.05

Document History

Date	Version	Editor	Change
10/09/2017	1.02	Oleg Andrianov	Added clarification regarding installation process
30/09/2017	1.03	Oleg Andrianov	Referenced KSC installation assumption
22/01/2018	1.04	Oleg Andrianov	Clarified p. 4.4.2.2.
June 2018	1.05	Oleg Andrianov	Changes as part of maintenance process

Table of Contents

1 About this document

1.1 Terminology

Terms and acronyms, most of them specific to Kaspersky Endpoint Security products, shall be defined.

Term	Definition
BIOS	Basic Input/Output System
FDE	Full Disk Encryption
KES	Kaspersky Endpoint Security for Windows
KSC	Kaspersky Security Center
SSL	Communication secured by Transport Layer Security Protocol v.1.2.
Token	Secure device (smart card/Integrated Circuit Card) able to perform RSA encryption with private key

1.2 References

Reference	Document title	Document version
[ST]	Security Target for Kaspersky Endpoint Security for Windows	1.05
[UGD]	Kaspersky Endpoint Security for Windows User Manual	1.05

2 Introduction

This document describes necessary preparative procedures for putting **Kaspersky Endpoint Security for Windows (version 11.0.0.6499 AES256)** in certified secure state as required by [ST].

2.1 ST Reference

Security Target for Kaspersky Endpoint Security for Windows (Version 1.05).

2.2 Product Reference

Described product is the **Kaspersky Endpoint Security for Windows (version 11.0.0.6499 AES256)** developed by Kaspersky Lab.

2.3 Required Non-TOE hardware/software/firmware

2.3.1 Hardware

The TOE has to run on devices (usually personal computer systems) with the following minimum requirements:

Processor: Intel Core i3 Duo 3.10GHz or equivalent

RAM: 2GB of free RAM

HDD: 2GB of available hard disk space

Network connection peripherals

2.3.2 Software

The Full Disk Encryption of Kaspersky Endpoint Security under this evaluation is provided for the following operating systems:

- Microsoft Windows 10 Professional x86 / x64;
- Microsoft Windows 10 Enterprise x86 / x64;
- Microsoft Windows 8.1 Enterprise x86 / x64;
- Microsoft Windows 8.1 Pro x86 / x64;
- Microsoft Windows 8 Pro x86 / x64;
- Microsoft Windows 8 Enterprise x86 / x64;
- Microsoft Windows 7 Professional x86 / x64 SP1;
- Microsoft Windows 7 Enterprise x86 / x64 SP1;

Kaspersky Endpoint Security – Full Disk Encryption works with the following file systems under Windows: FAT, FAT32, and NTFS4.

Additional requirements for Full Disk Encryption Functionality:

- Different drives for the loader and the operating system are not supported.
- Basic disk partitions are supported. Dynamic disk partitions are not supported.
- At least 2 % of contiguous free disk space shall be available on the disk for encryption.

2.3.3 KSC management software

Kaspersky Security Center 10 (version SP3 or later) have to be installed. You may obtain KSC installation package and documentation from the Kaspersky Lab website: http://support.kaspersky.com/ksc10#downloads

3 Security Objectives

Following requirements have to be met for secure operation of the TOE.

3.1 KSC management

As per [ST] Security Objectives for the Operational Environment KSC have to be installed and configured to enable administration of TOE.

The KSC server shall be located in a trusted environment that provides strong physical and logical access restrictions. The interaction of integrated security measures in the KSC server environment ensures the needed quality, integrity and confidentiality of the relevant cryptographic material and keys stored on the server.

The TOE and the KSC server communicate using a secure SSL connection that is provided by the environment. The NetAgent of the KES has to be used. The NetAgent SSL connection has to be configured to provide a strong server authentication together with strong encryption and integrity protection of all transmitted data.

3.2 TOE secure operation

Non-trusted software (especially with ability to perform direct access to the hard disk) is not installed and will not be installed on the device secured by the TOE. The users are instructed not to install or use utility programs like partition managers or disk copy programs.

3.3 Trusted administration

The administrators responsible for the device and KSC server administration have to be trustworthy. They need to study guidance for KSC and TOE and perform all tasks correctly regarding the TOE security.

3.4 Correct behaviour of authorised users

Authorised users shall not actively compromise the security of the device secured by the TOE and the TOE itself and should be instructed not to leave a device secured by the TOE while it is switched on and running.

4 Preparative procedures

4.1 OS setup

4.1.1 Secure Boot has to be enabled on supported systems

Please refer to device manual for instructions.

4.1.2 Safe mode boot for OS is disabled

Please refer to OS documentation for instructions.

4.2 Check installation package

Obtain installation package from Kaspresky Lab support website (https://support.kaspersky.com/14898).

Check hash sums of TOE with listed in the ST to make sure you are using certified package.

You may use tools of your choice that support calculation of sha256 hash or CertUtil tool included into widows installation. In latter case you should use following command:

```
c:\>certutil -hashfile <path-to-file> sha256
```

Compare calculated hash to the one listed in Security Target and published on a Kaspersky website.

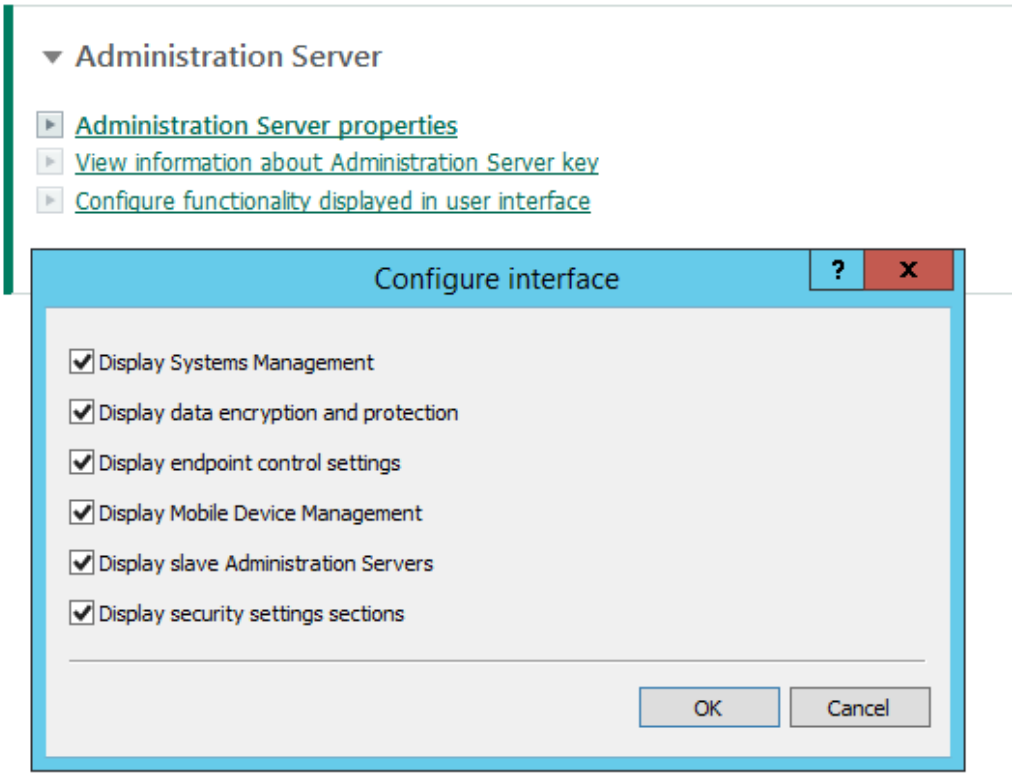
4.3 Kaspersky Security Center (KSC)

4.3.1 KSC installation

Make sure Kaspersky Security Center 10 (version SP3 or later) is installed in secure environment as per 3.1 and configured in secure manner.

4.3.2 KSC settings

Use following setting in KSC Interface to display encryption and control functionality.

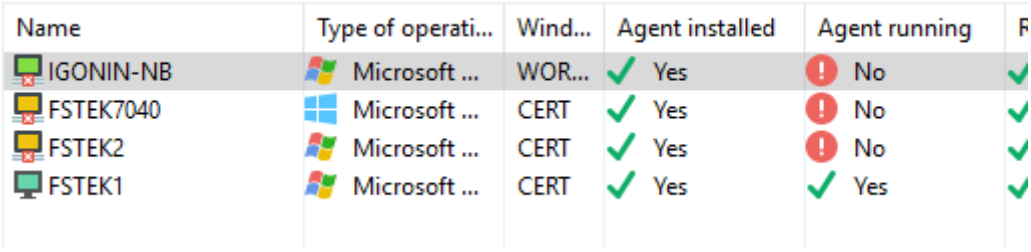


4.3.3 Set up KSC Connection.

Install KSC Network Agent on endpoint machines that will be protected by the TOE and setup connection to KSC.

Make sure connection is secured using SSL. Nagent will download KSC digital certificate on first connection, or you can provide this manually. Refer to Annex 3 for details.

Check that all machines have “Agent installed” mark shown in KSC interface as shown below.



4.3.4 Install management plugin

On the device with Administration Console installed, run the klcfginst.exe file, which is included in the KES distribution package.

4.4 Product Installation

4.4.1 Manual installation

You may install TOE manually on selected machines using interactive setup process. Installation walkthrough is included in Annex 1.

4.4.1.1 Make sure to install necessary components

Choose Custom installation in setup options

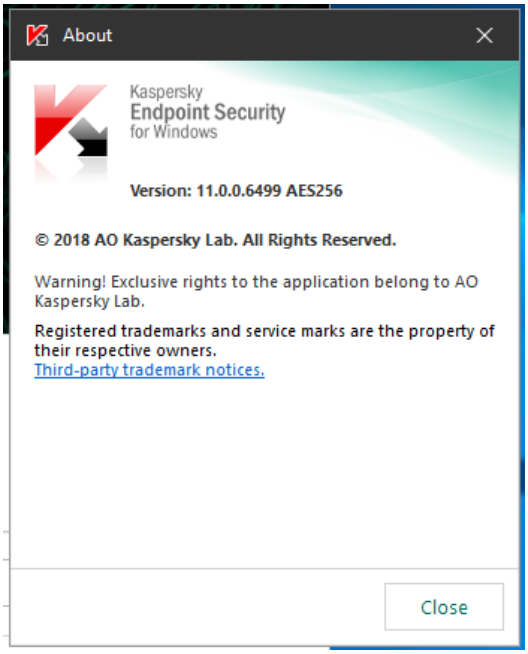
Make sure “Drive Encryption” option is checked.

4.4.1.2 Install into directory recommended by setup process

Do not change installation directory proposed by installation process.

4.4.1.3 Check Version of installed product

Use menu “About” in product GUI to verify TOE version installed is 11.0.0.6499 AES256.



4.4.2 Remote installation

You may install TOE in an automated way using KSC to managed endpoints. Installation walkthrough is included in Annex 2.

4.4.2.1 Create installation package and task

Process is described in Annex 2.

4.4.2.2 Check version

After task is completed you may check that version was by checking on each protected machine as described in p. 4.4.1.3.

4.4.3 Install activation keys

If you have not included activation information on steps 4.4.1 or 4.4.2.1 you should do this now. Refer to [UGD] section 'Key addition task settings section" for instructions on how to import and rollout activation keys. Imported keys should be able to activate KES10 encryption functionality. Keys have to be rolled out to endpoint machines. You may use "Key usage report" in KSC to verify that this step was done correctly. All protected machines have to be activated.

4.4.4 Upgrade from previous version

You can upgrade Kaspersky Endpoint Security 10 for Windows with Kaspersky Full Disk Encryption 3.0 (version 10.3.0.6294 AES256) to Kaspersky Endpoint Security for Windows (version 11.0.0.6499 AES256) by installing TOE as described above. Previous version will be automatically removed and replaced by new TOE version.

You must decrypt all hard drives before upgrading. Upgrade will not proceed if there are encrypted drives.

4.5 Set up policies for Kaspersky Endpoint Security for Windows

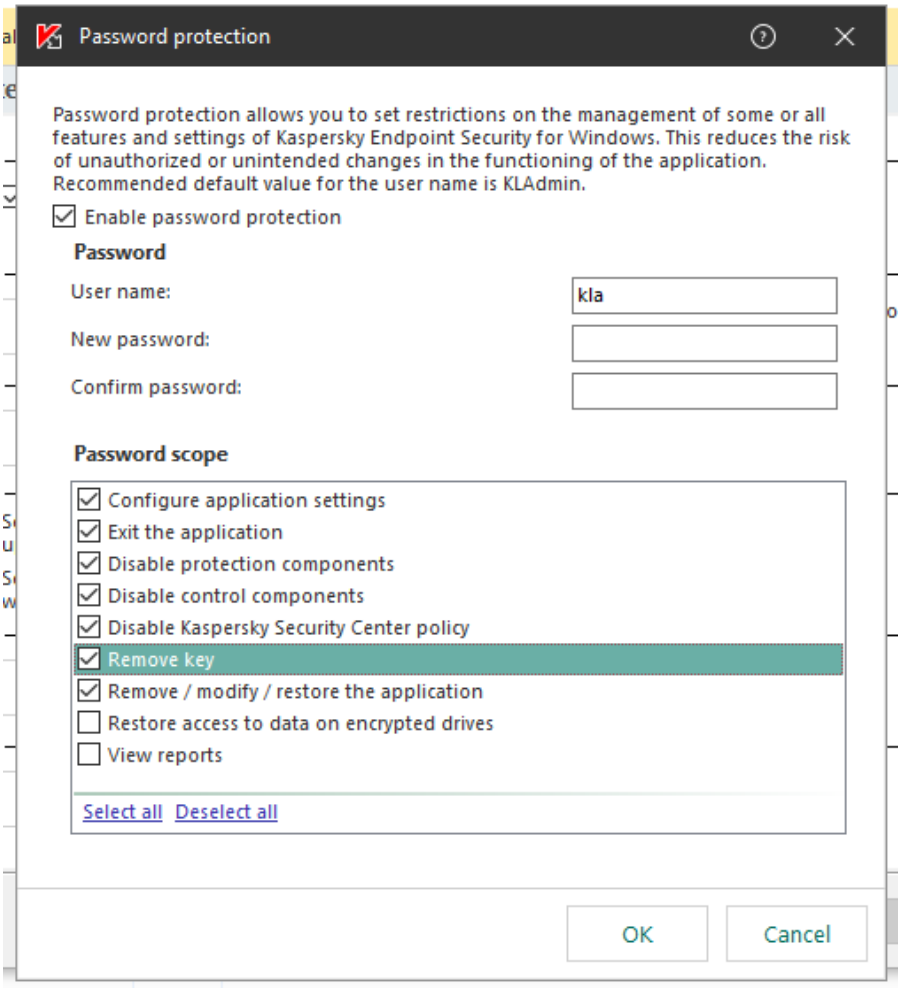
Refer to section "Remote administration of the application through Kaspersky Security Center" in [UGD] documents for help when creating policies for Kaspersky Endpoint Security for Windows in KSC.

You must create a valid active policy for managed computers, running TOE.

4.5.1 Setup settings password protection

Make sure you use a secure password. While product uses salt to minimize rainbow-tables attacks choose password complexity matching current best practices –currently a random set of characters of 10+ length.

Make sure the scope of password protection at least covers the following:

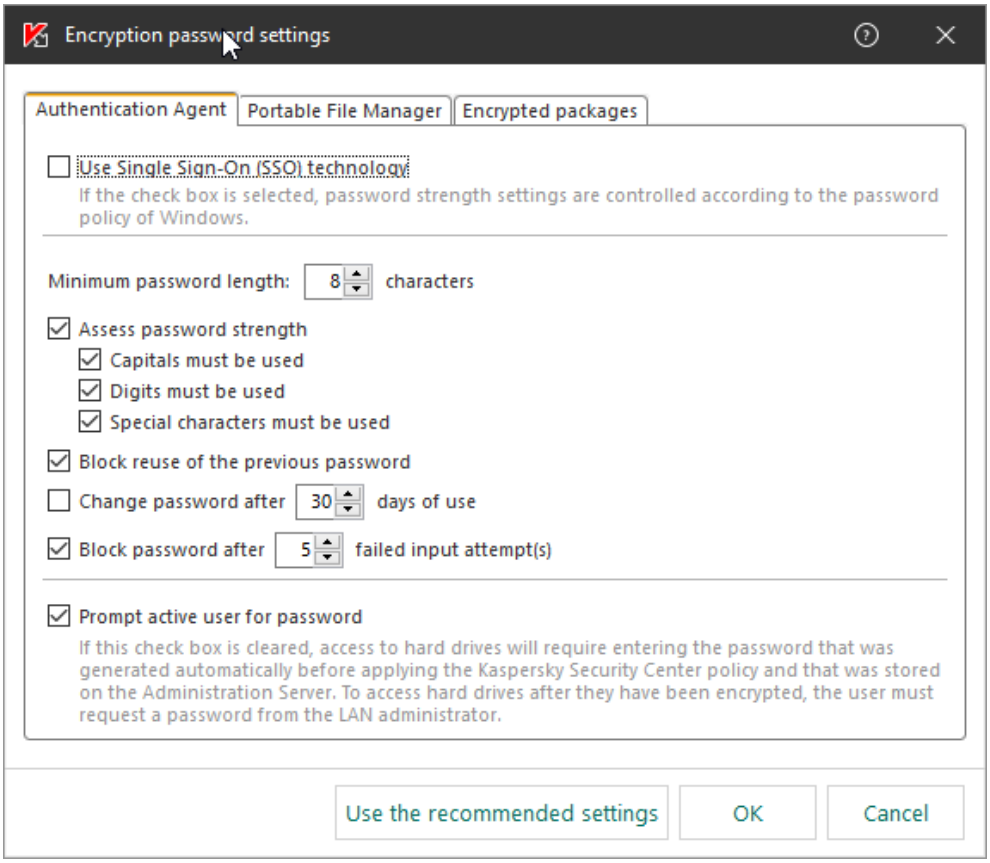


4.5.2 Create encryption policy

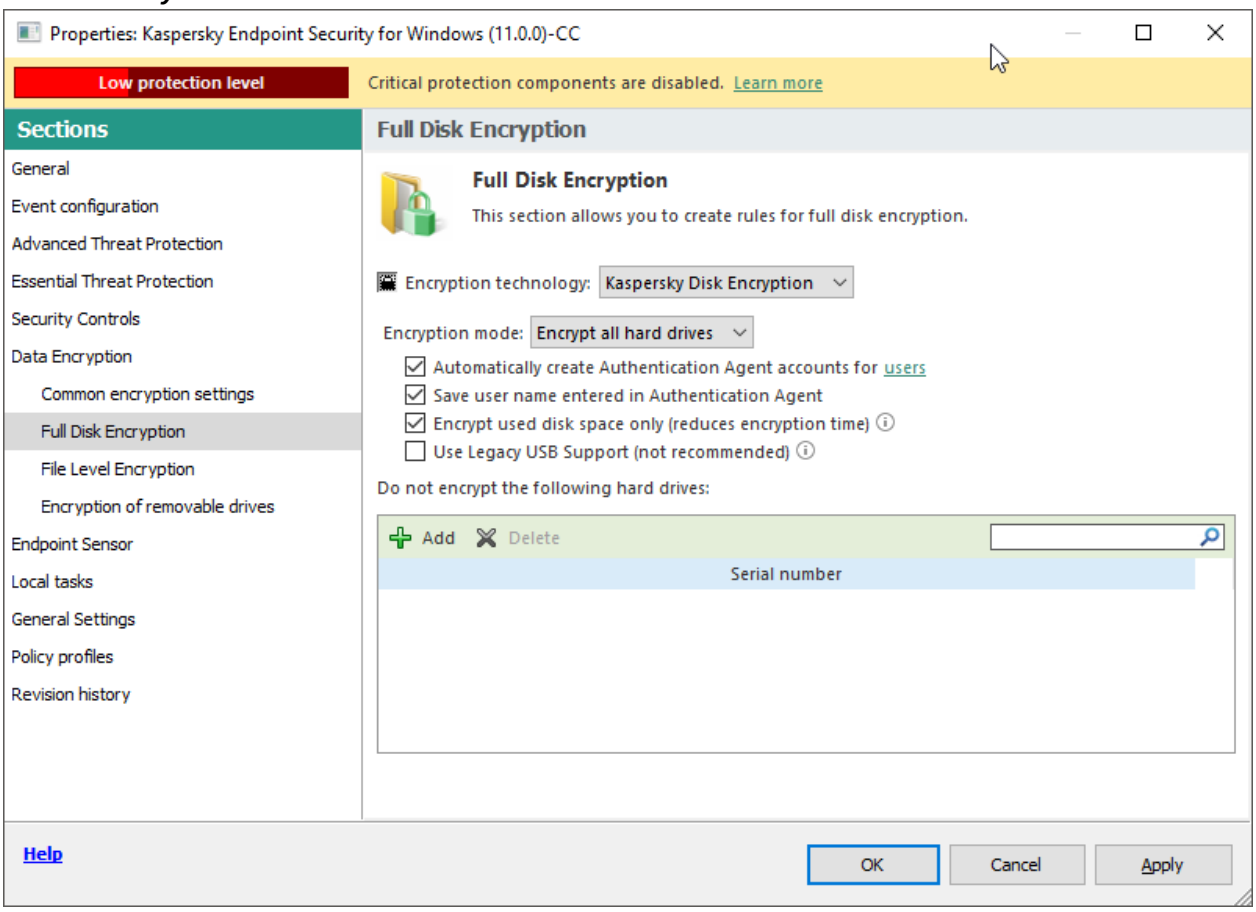
See [UGD], Data Encryption section for more details and explanation of this.

4.5.2.1 Policy should have Single Sign On feature disabled

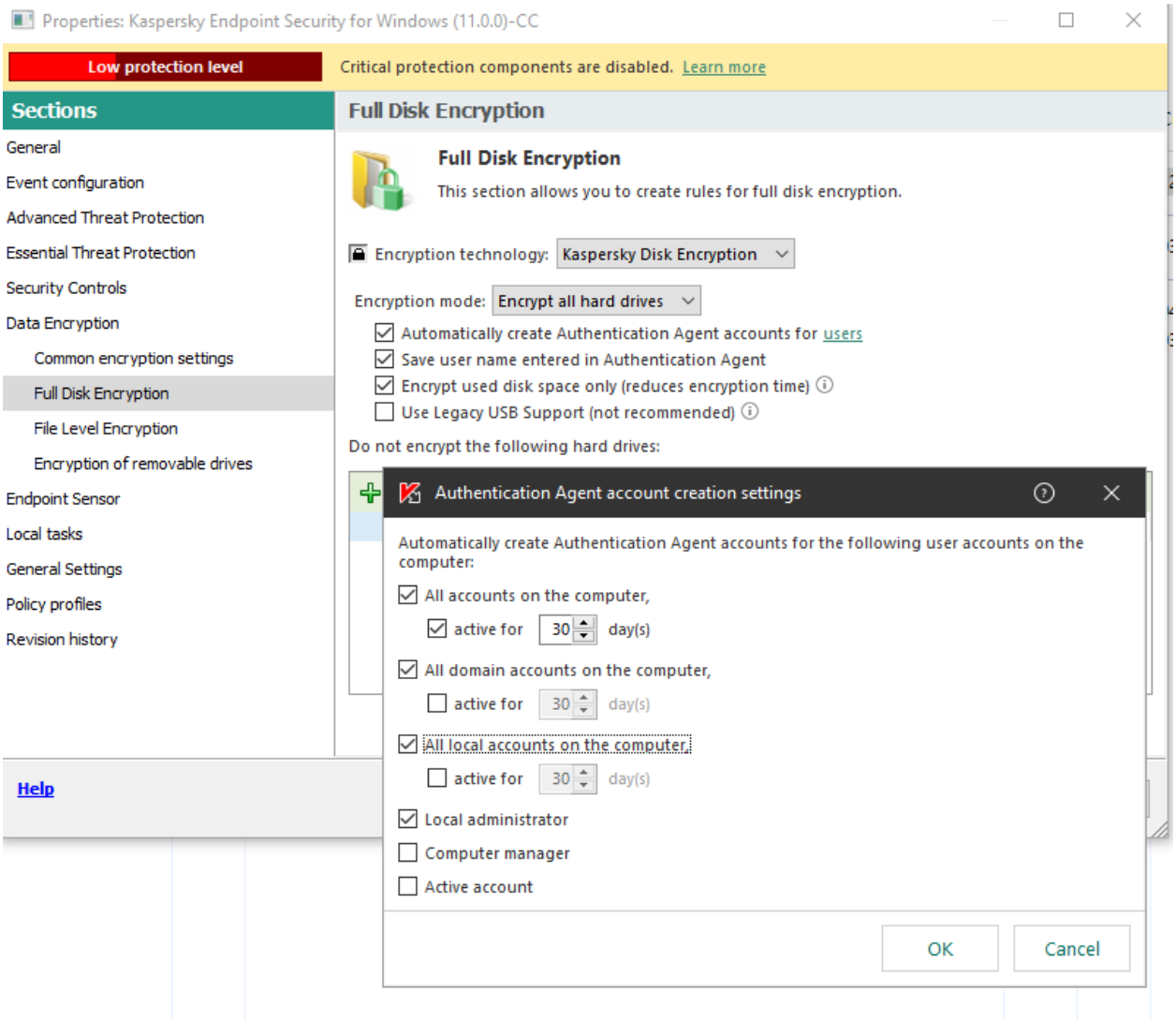
See [UGD], p.278.



4.5.2.2 Policy should cover all hard disk

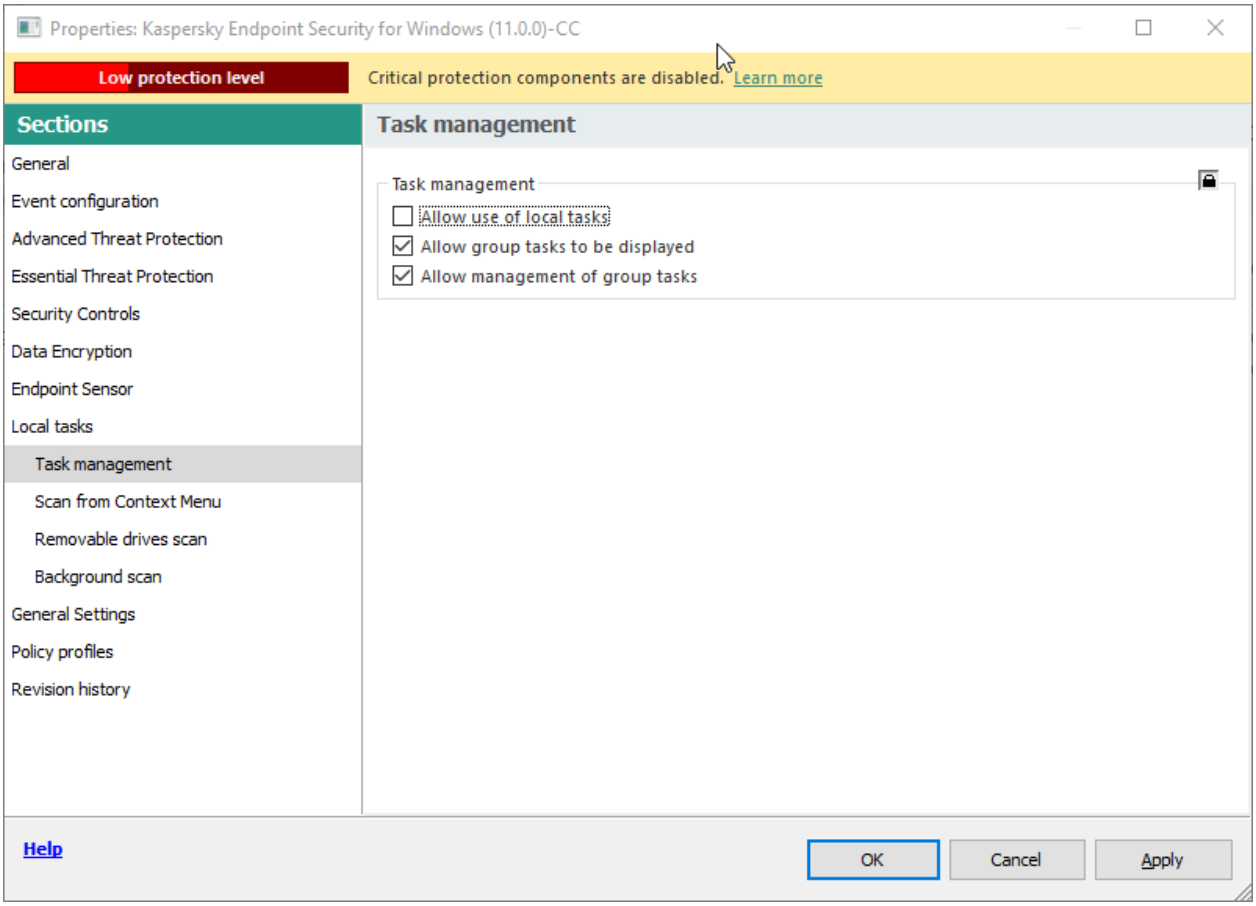


4.5.2.3 Encryption task should create accounts for users



4.5.3 Disable local Tasks

Disable local update tasks by unchecking *Allow use of local tasks* in **Task Management** parameter section in **Local tasks** section of policies.



4.6 Configure organization-specific settings.

You may alter Policy created in section 4.5 policy to meet your organizational rules and policies.

4.6.1 Create relevant access policies

Create policies for Application Startup Control, Web Access Control, Device Access Control that meet your organizational security policies, including specific set of rules TOE will enforce.

4.6.2 Create AV settings

Check and alter if needed settings for AV functions of product, that meet your organizational security policies, including relevant actions or exclusions.

4.6.3 Group tasks

Create group tasks for different AV scans that users will be able to execute manually.

4.7 Apply policies for Kaspersky Endpoint Security for Windows

4.7.1 Apply created policy

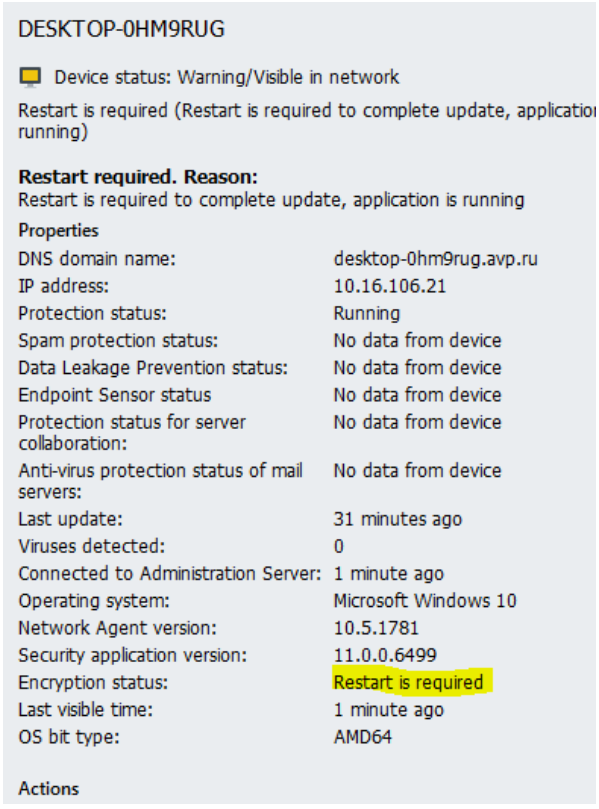
You need to enforce Policy created in previous sections to managed machines. Refer to [UGD] for instructions.

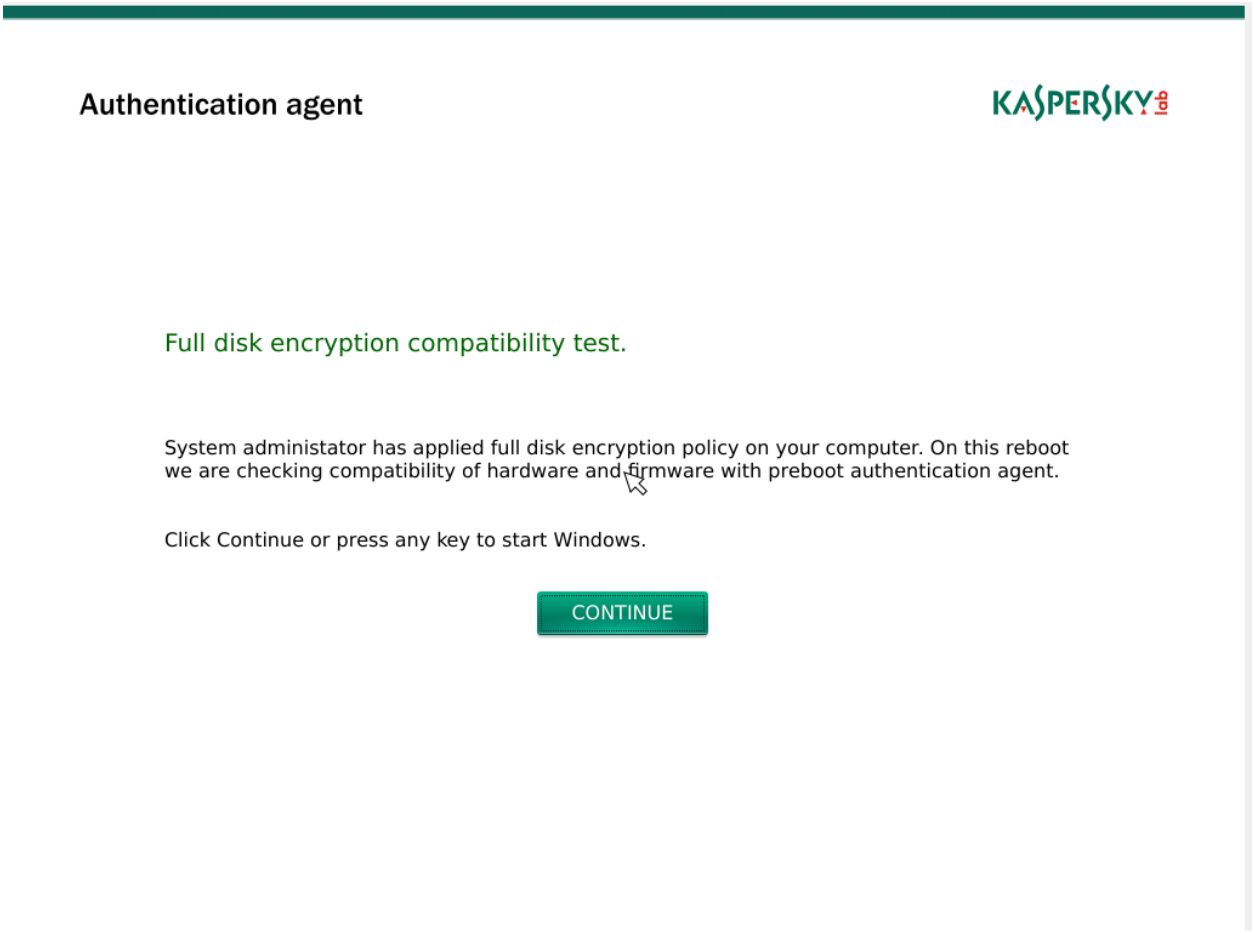
You may check policy enforcement in a Policies window for managed machines.

4.7.2 Verify that encryption tasks are finished on endpoint machines

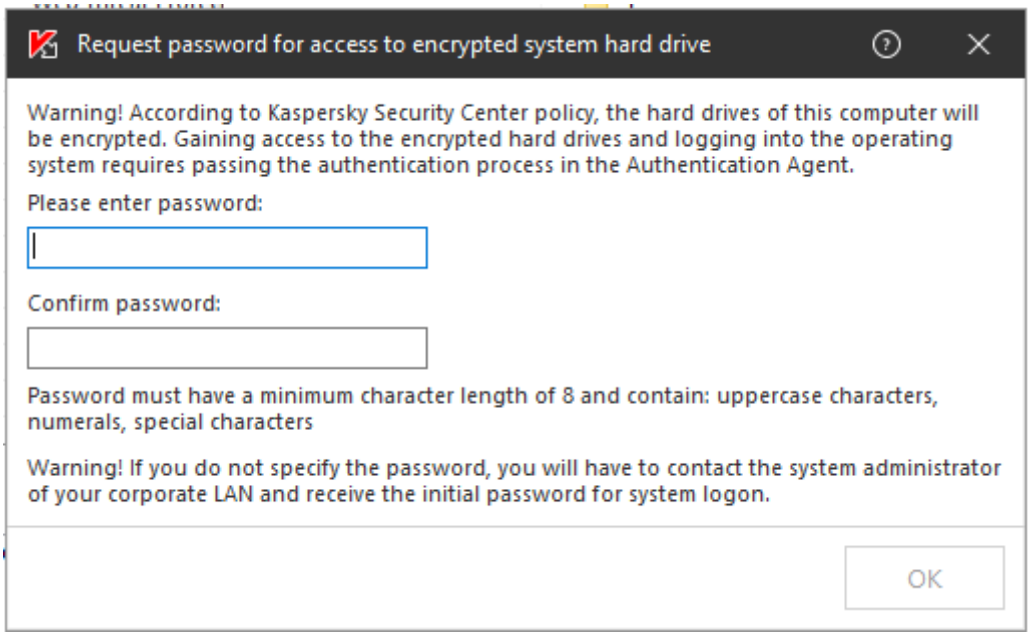
4.7.2.1 Endpoint pre-encryption check

It may be required to reboot target machines to conduct initial test of hardware compatibility



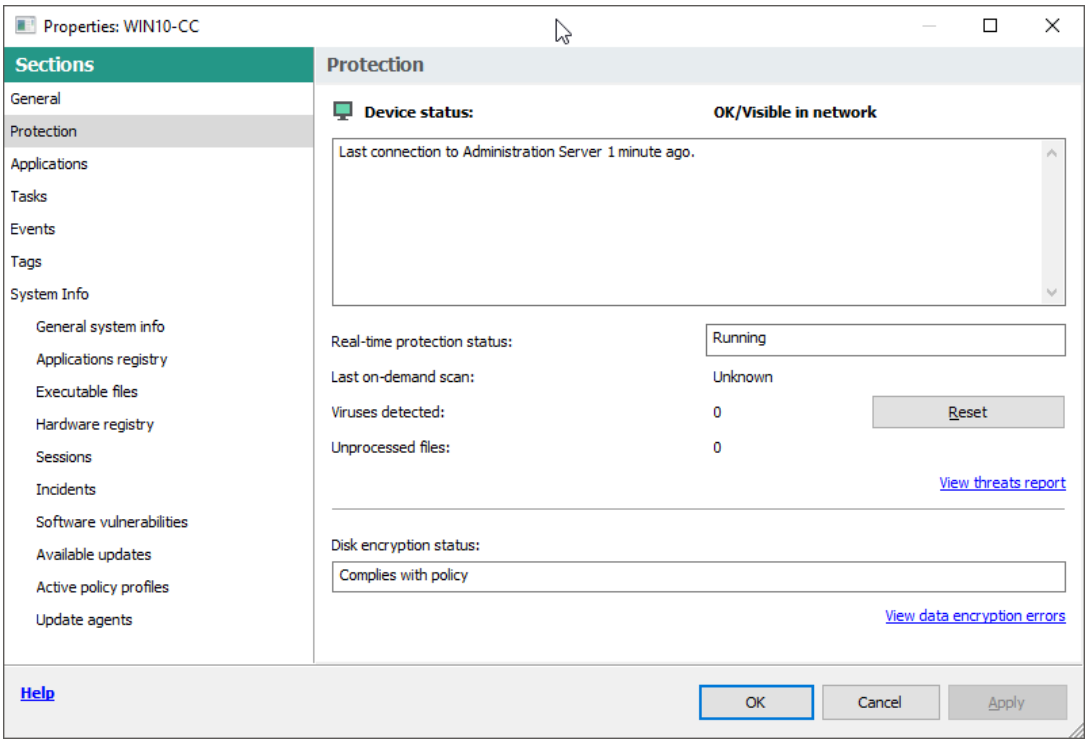


Users will then be prompted to enter password for encrypted drive.



4.7.2.2 Status of encryption

Encryption of hard drives takes time. You may view encryption status of machine in KSC using machine properties. Disk encryption status should be “Compiles with policy”



Until disk encryption is finished it is not considered correctly secured.

4.8 Create tasks for managed computer running Kaspersky Endpoint Security for Windows

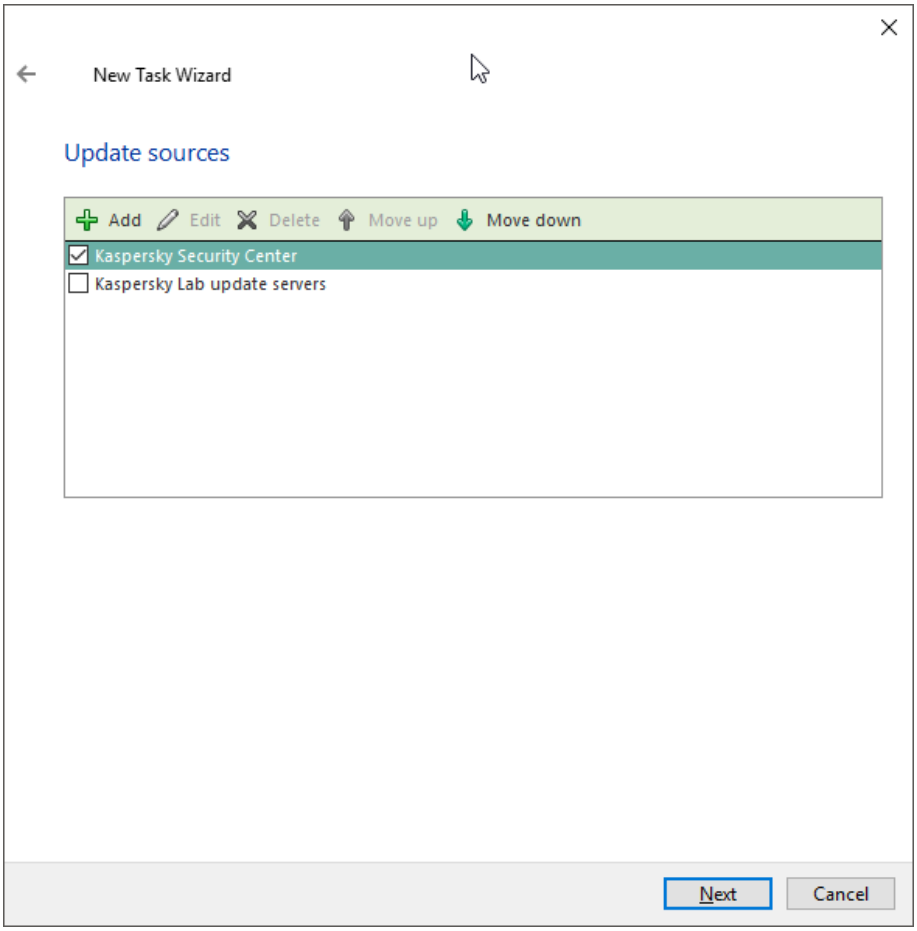
4.8.1 Create group tasks

You can create tasks that will be performed by Kaspersky Endpoint Security for Windows on schedule or by user commands. Refer to [UGD] for details.

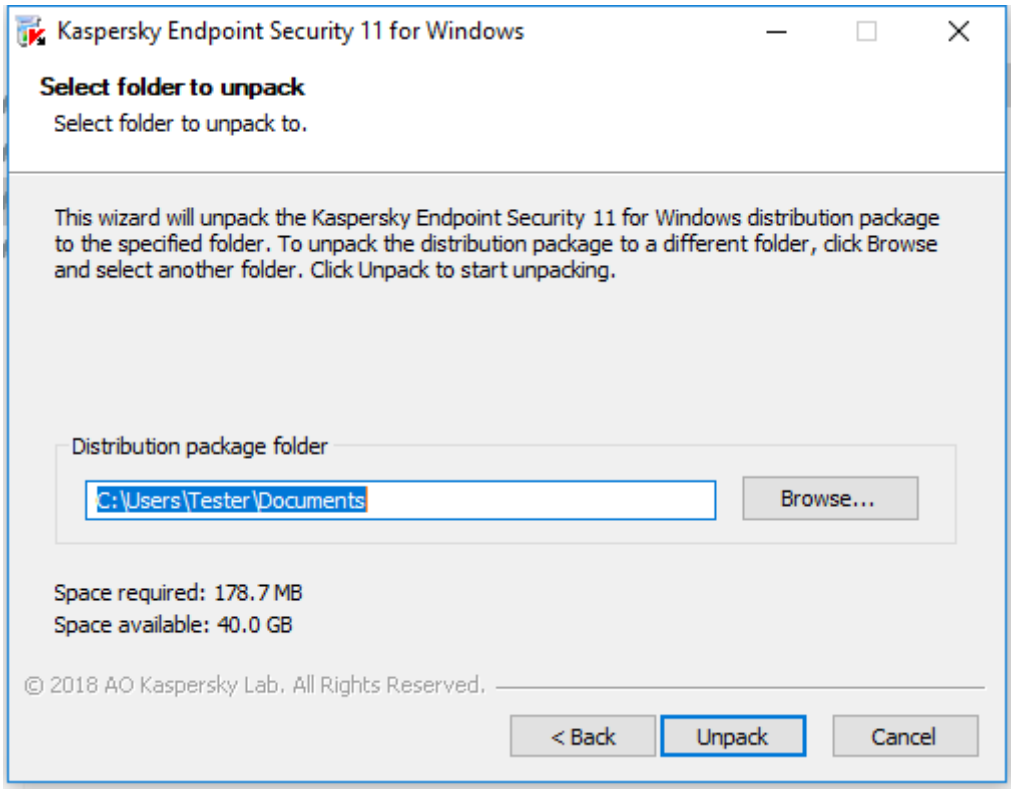
4.8.2 Modify existing Update task to disable AV updates[1]

Locate existing Update task in KSC and modify it to enable only update through KSC repository.

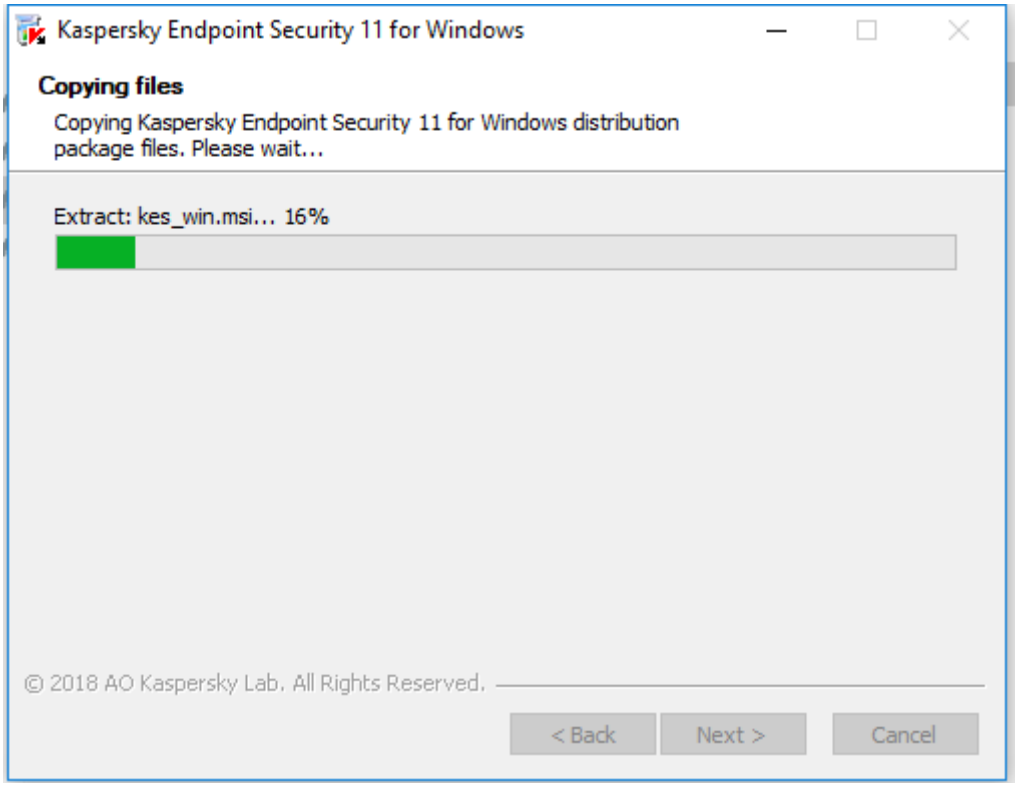
[1] As AV updates include updated program modules that might affect program behavior they are not permitted in certified product state.


New Task Wizard
Update sources
Add
Edit
Delete
Move up
Move down
Kaspersky Security Center
Kaspersky Lab update servers
Next
Cancel

Annex 1. Installation walkthrough



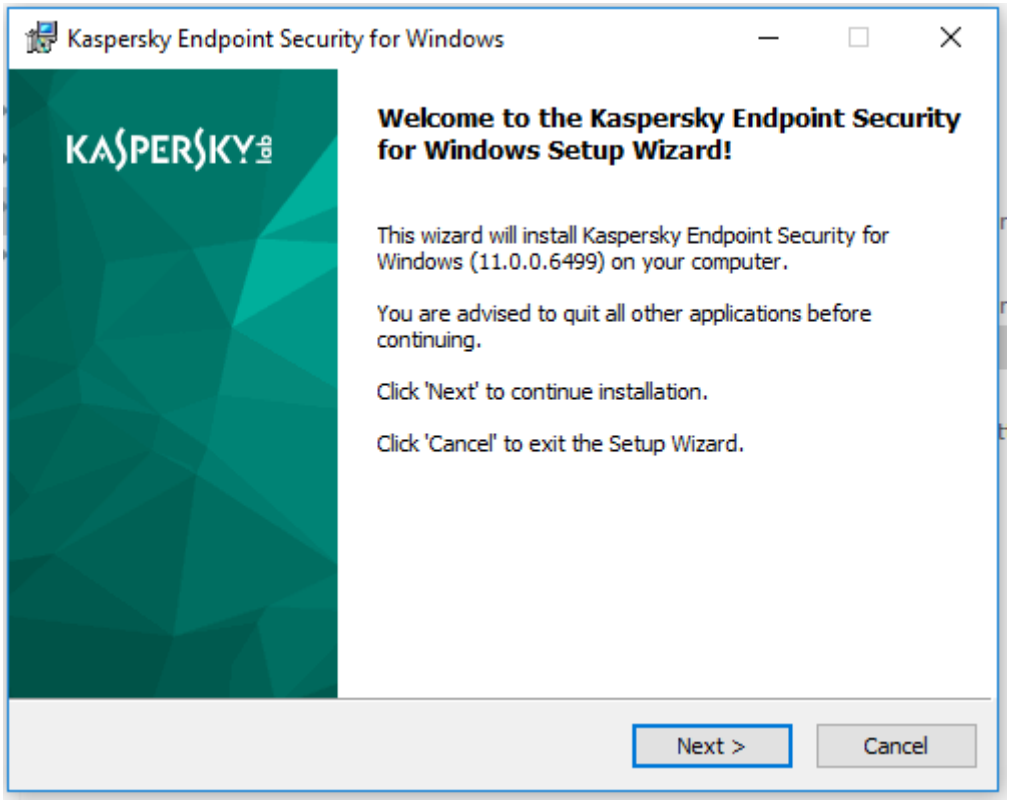
Choose temporary directory to wich the installation package will be extracted before installation.



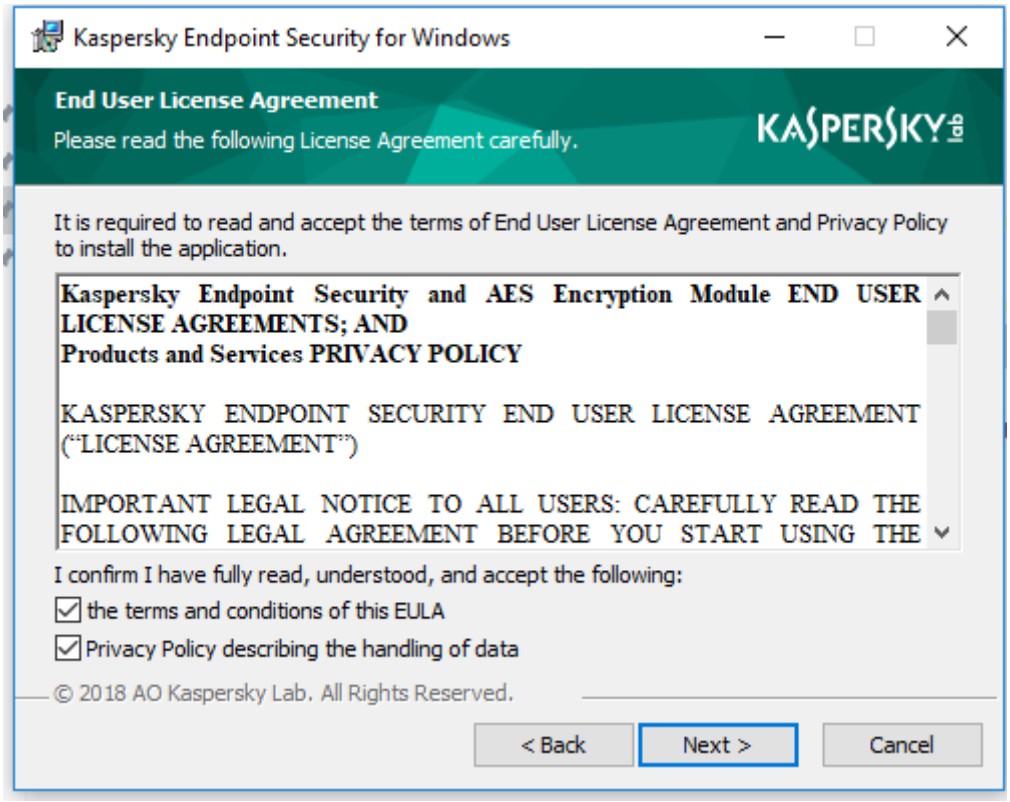
Navigate to the temporary folder created earlier and run Setup.exe.

Acept the UAC warning if shown.

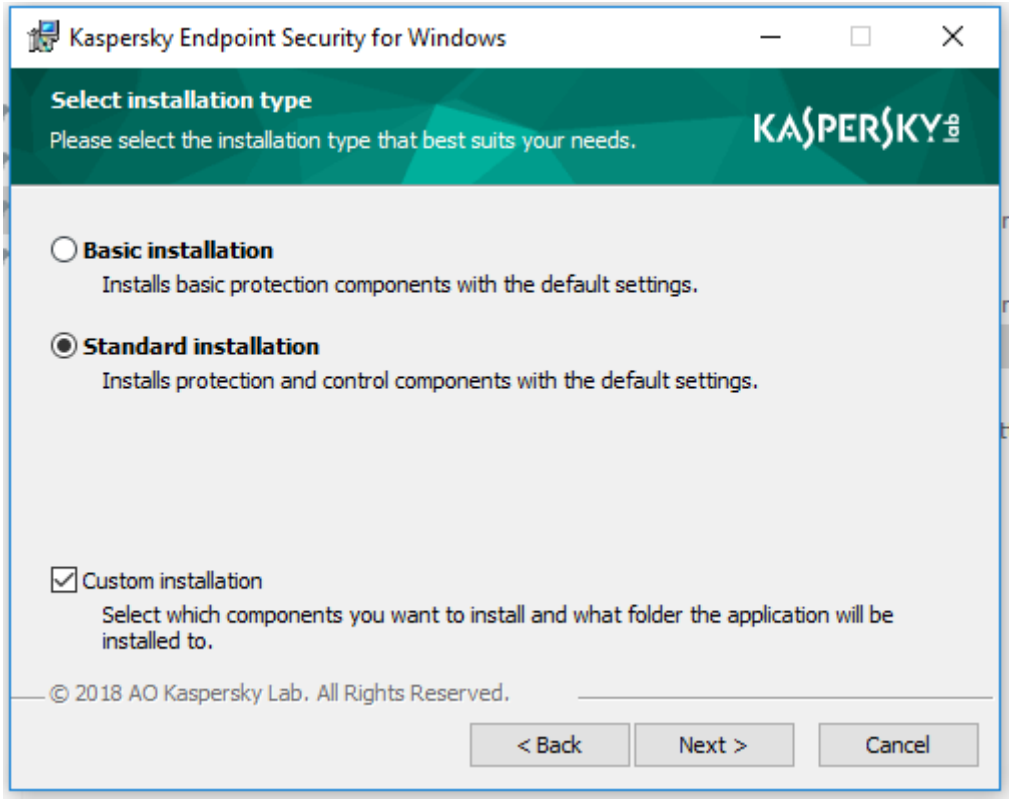
Setup will start.



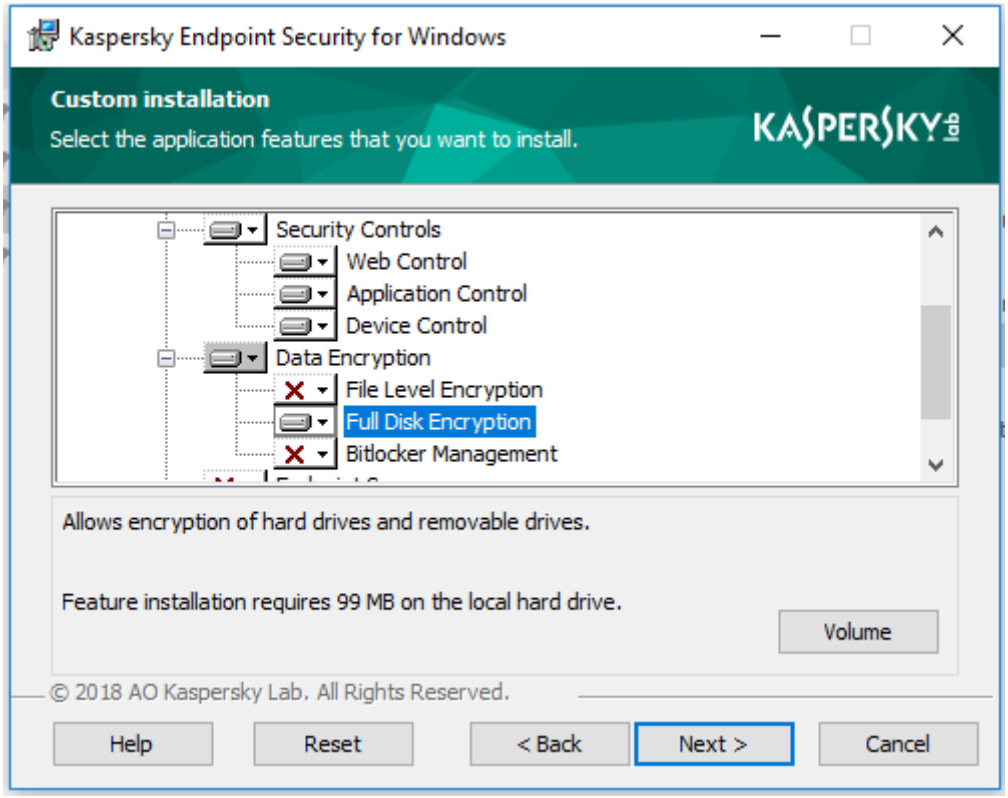
Read and accept End User License Agreement.



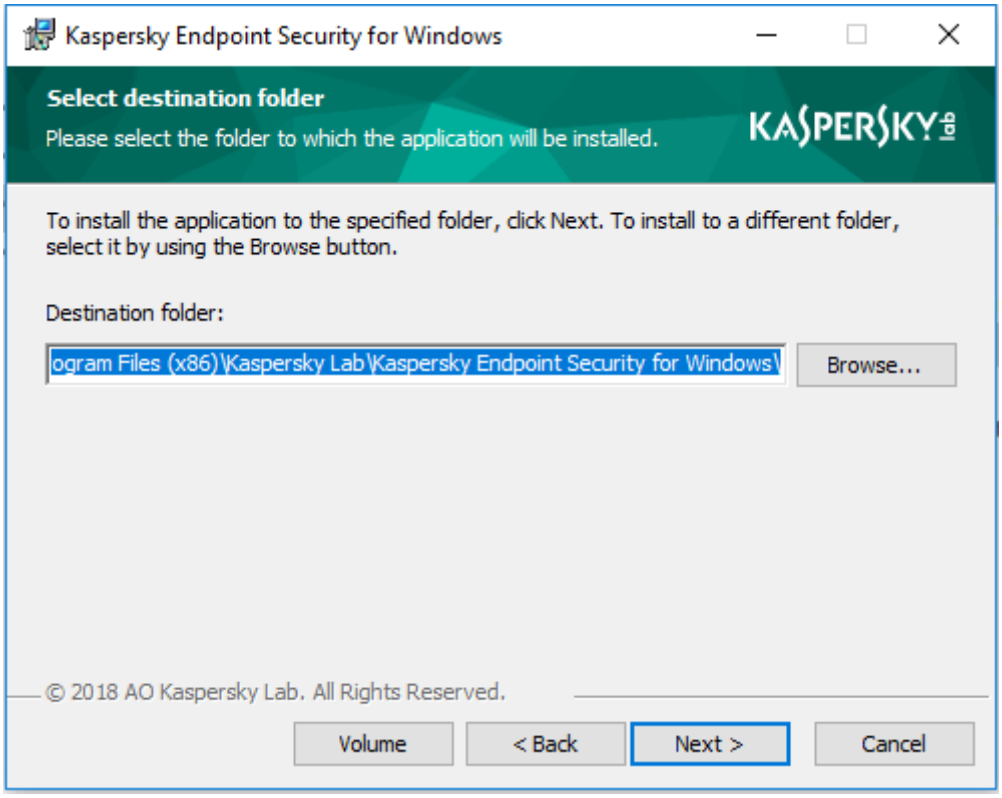
Make sure you choose Custom Installation option.



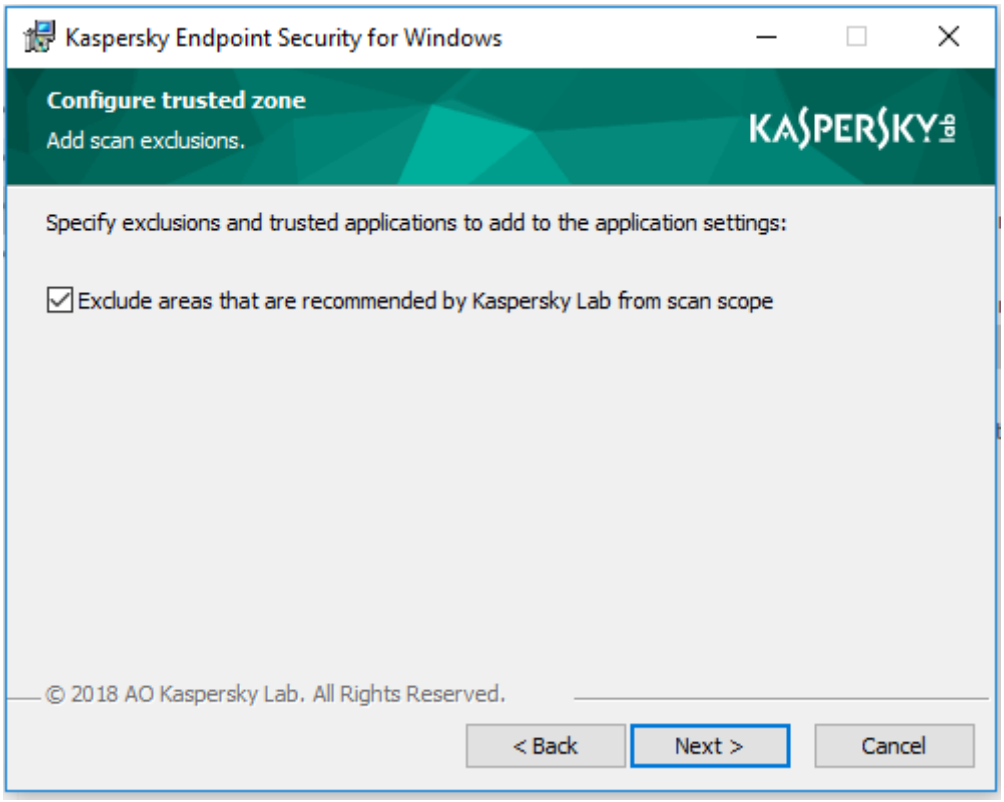
In the next screen scroll down and choose “Drive Encryption” option to de installed.



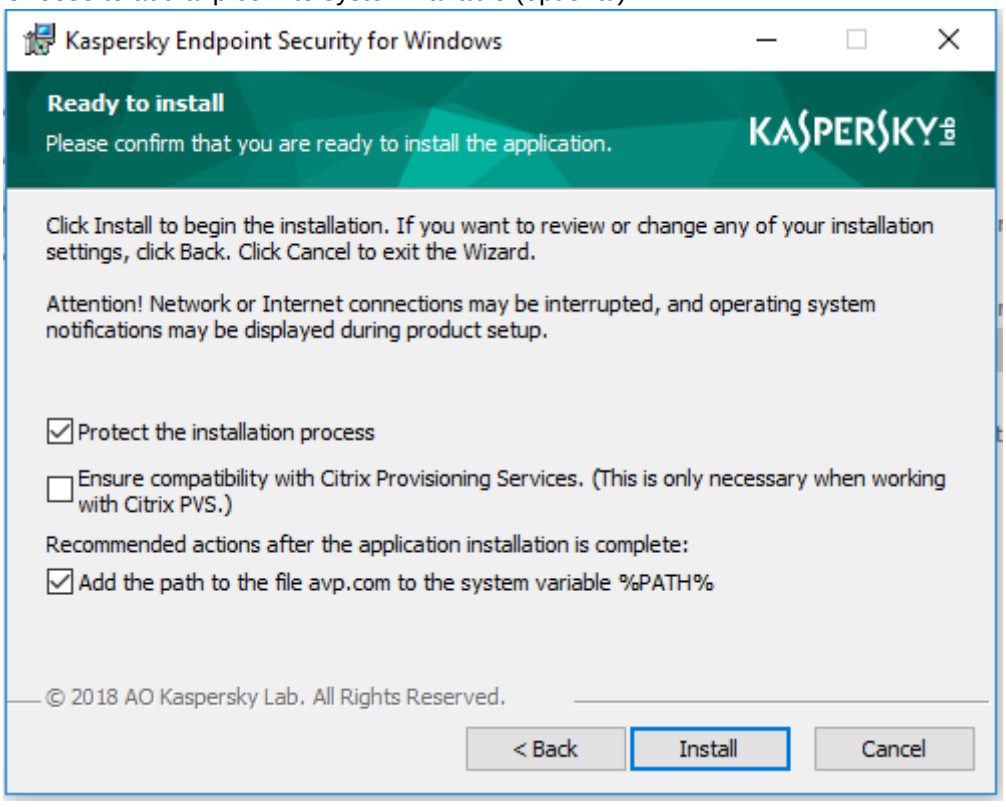
Leave destination folder as offered by the setup.



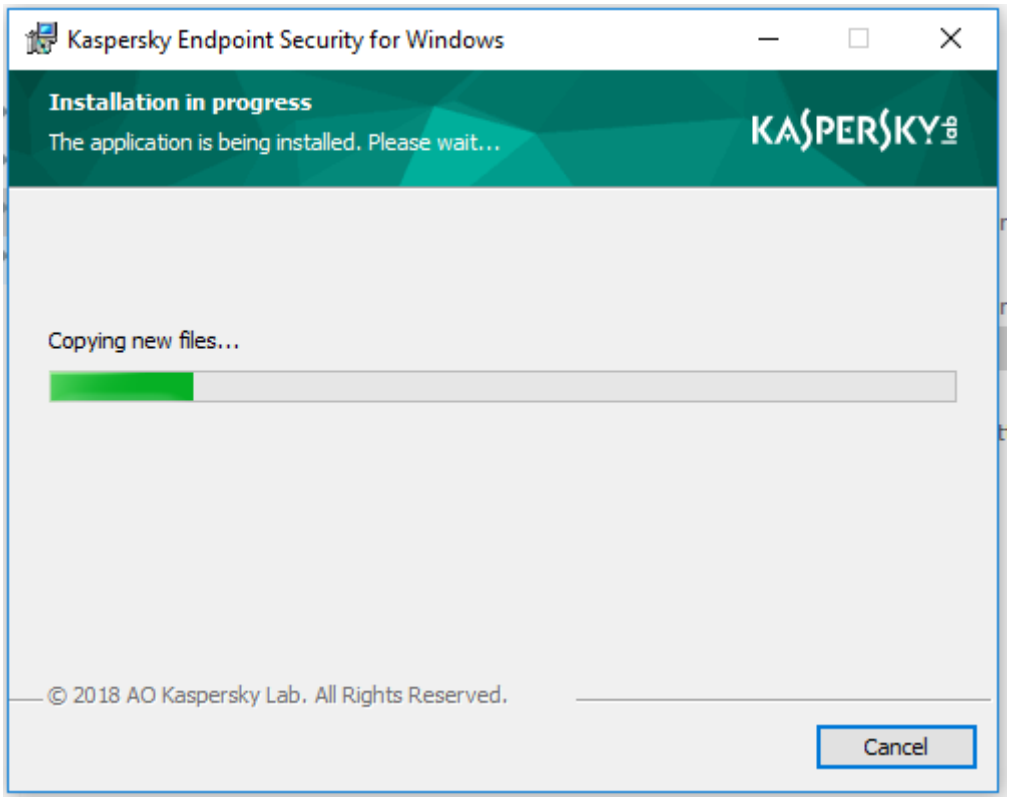
Leave suggested exclutions checked (you will be able to change this later according to your organizational policies).



Choose to add avp.com to system variable (optional).

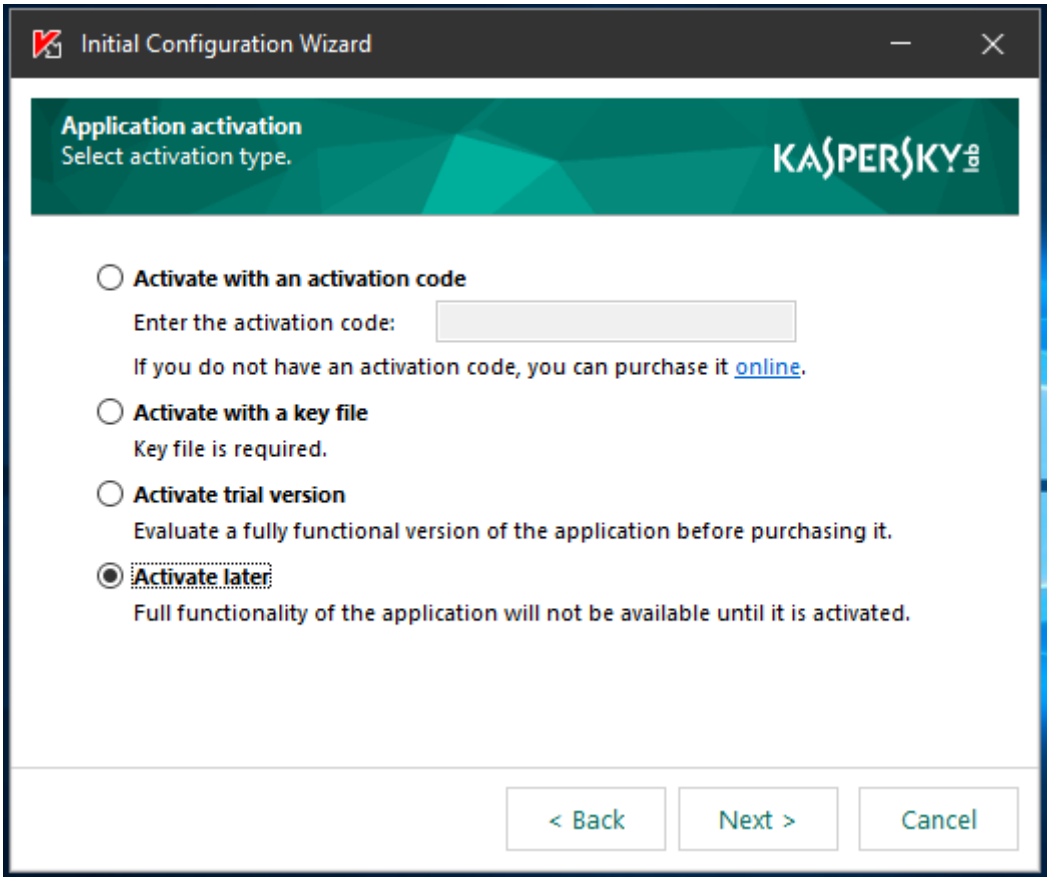


Installation process will begin.

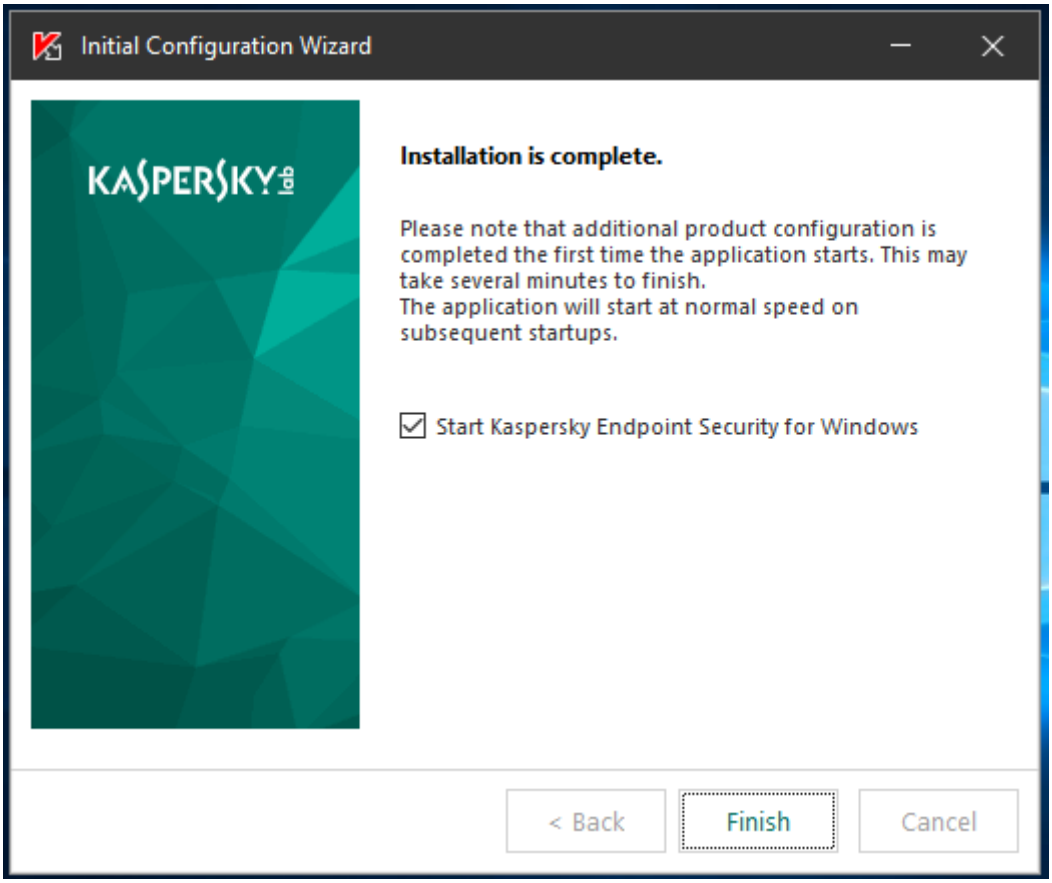


After installation configuration wizard will start:

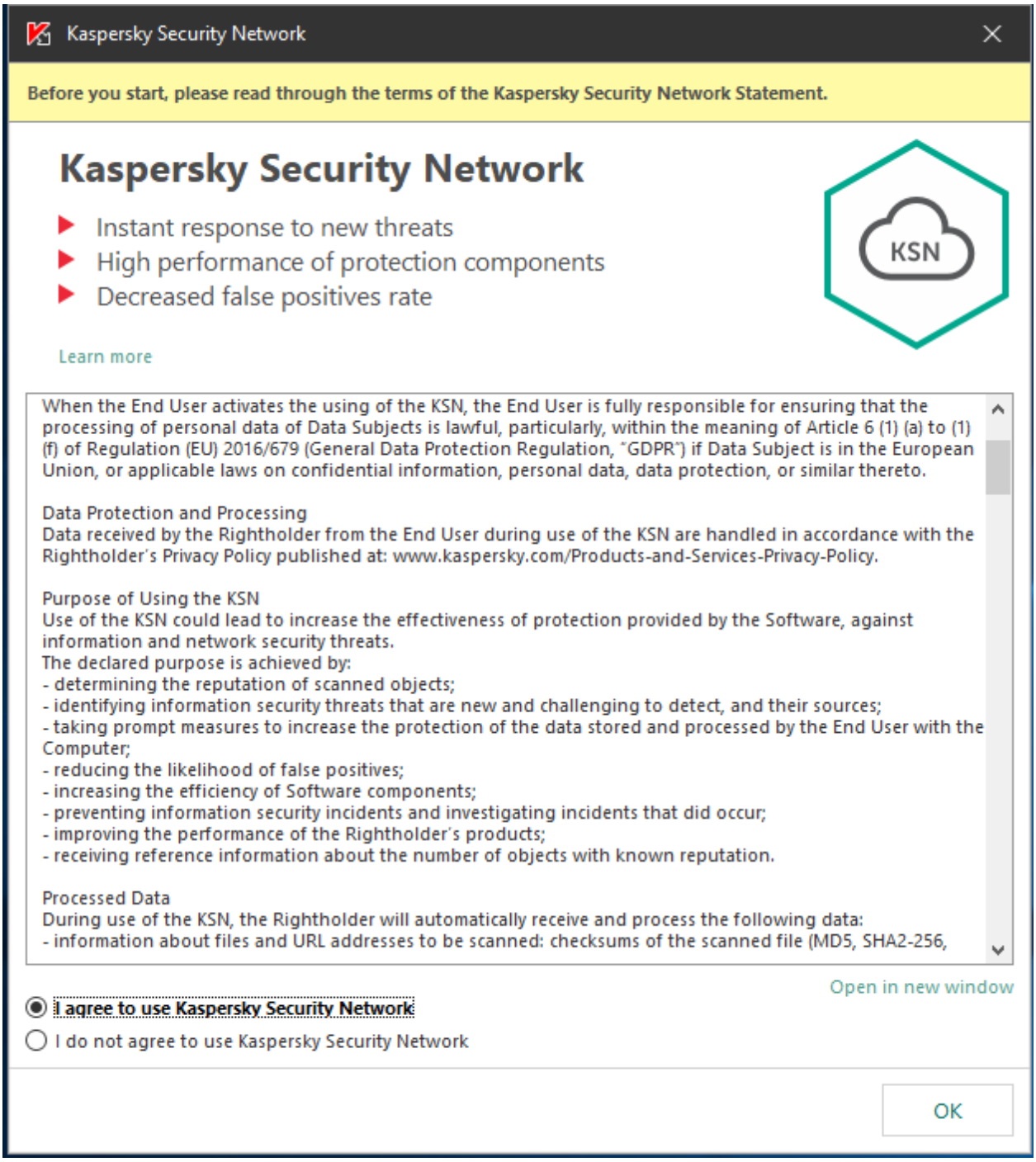
Product will ask for Activation.You may enter you activation code or key here or add Activate later through KSC (see step 4.4.3) In latter case you may choose “Activate Later” option.



After lincese was added, you will see final screen:



After you click Finish product will be started and KSN agreement will be displayed.



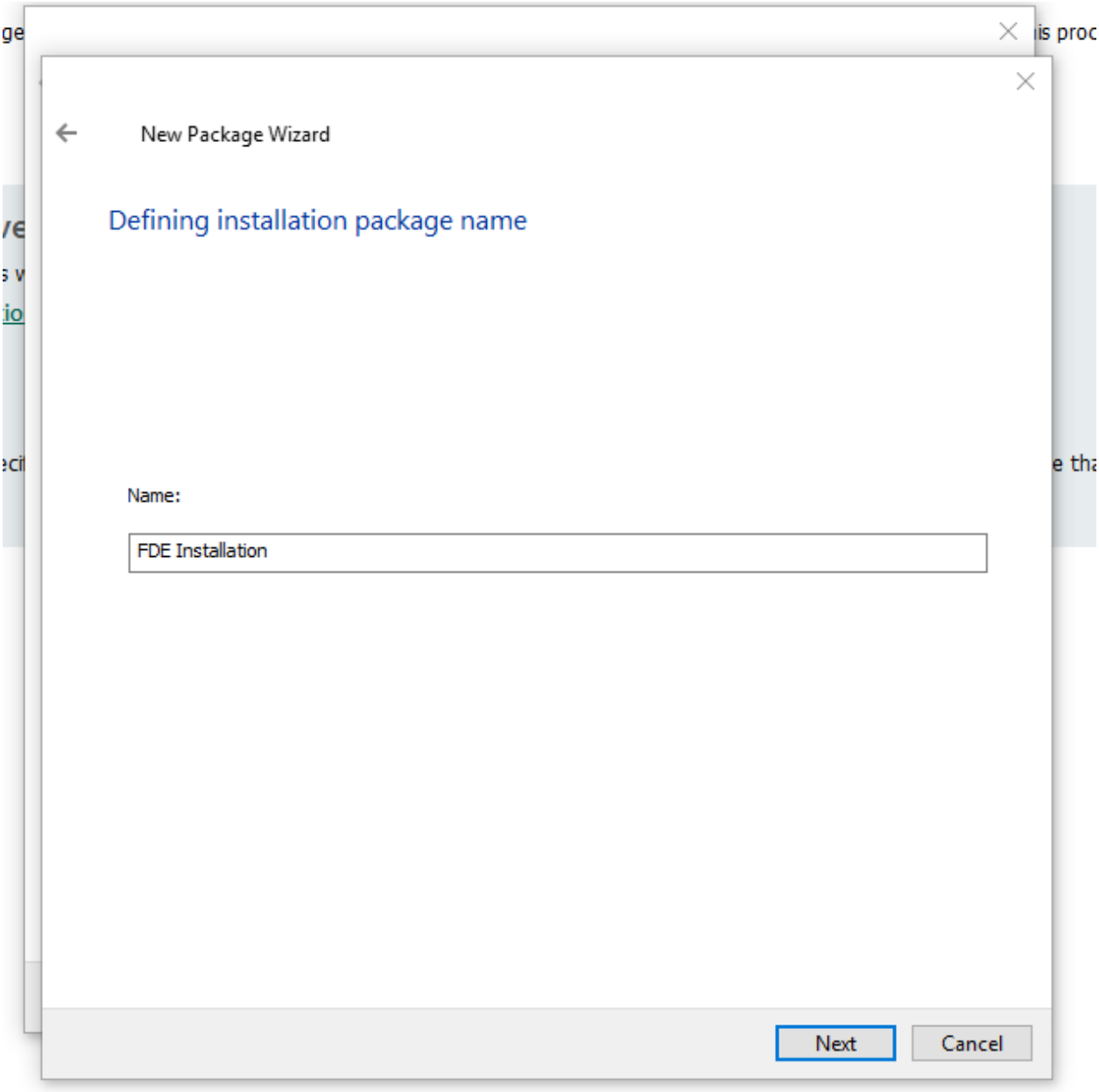
After you accept (or not accept) the agreement based on you company policies, the TOE will be running and protecting the system).

Annex 2. Remote Installation

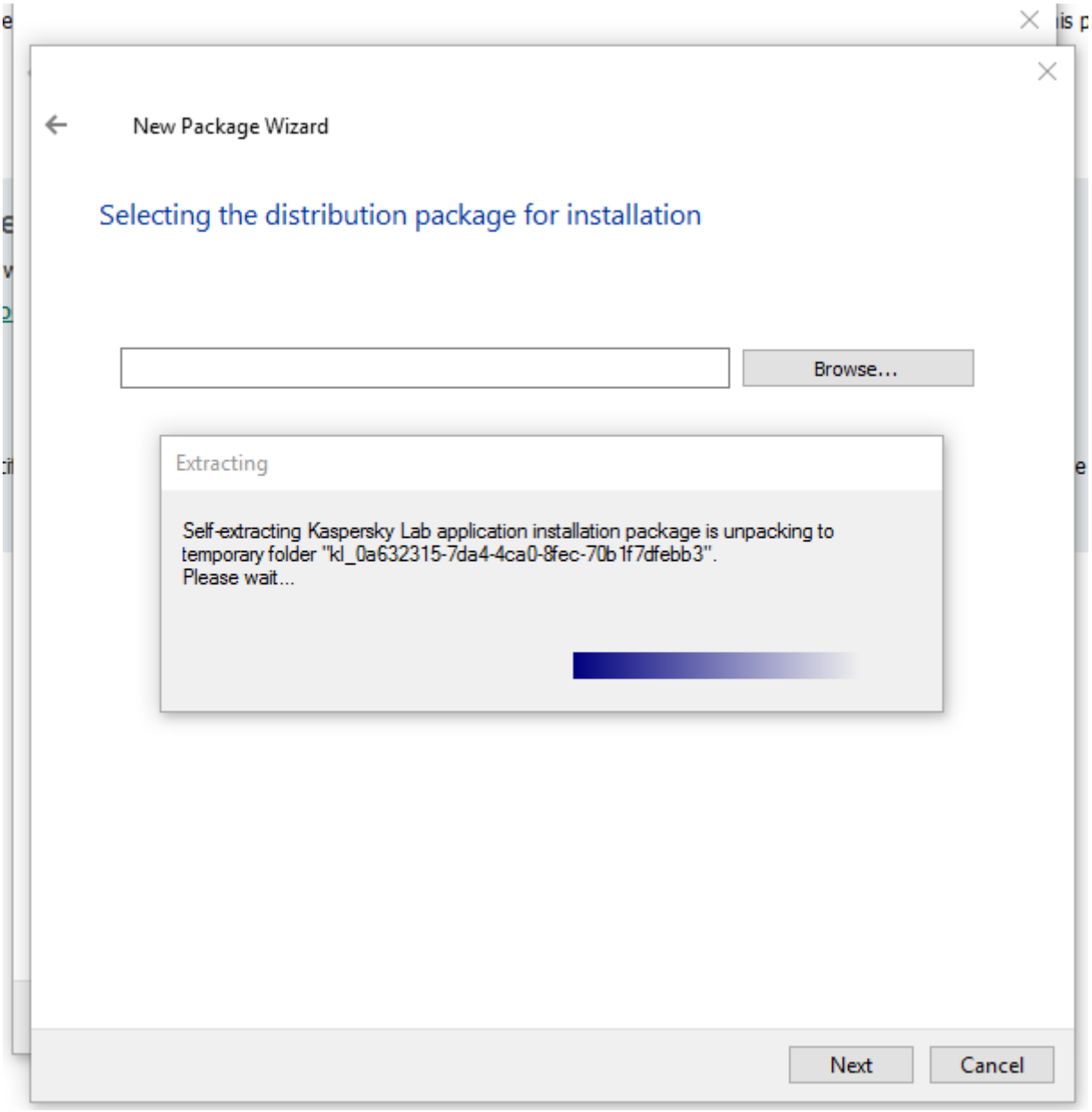
Process is done in KSC.

First you need to create Installation package.

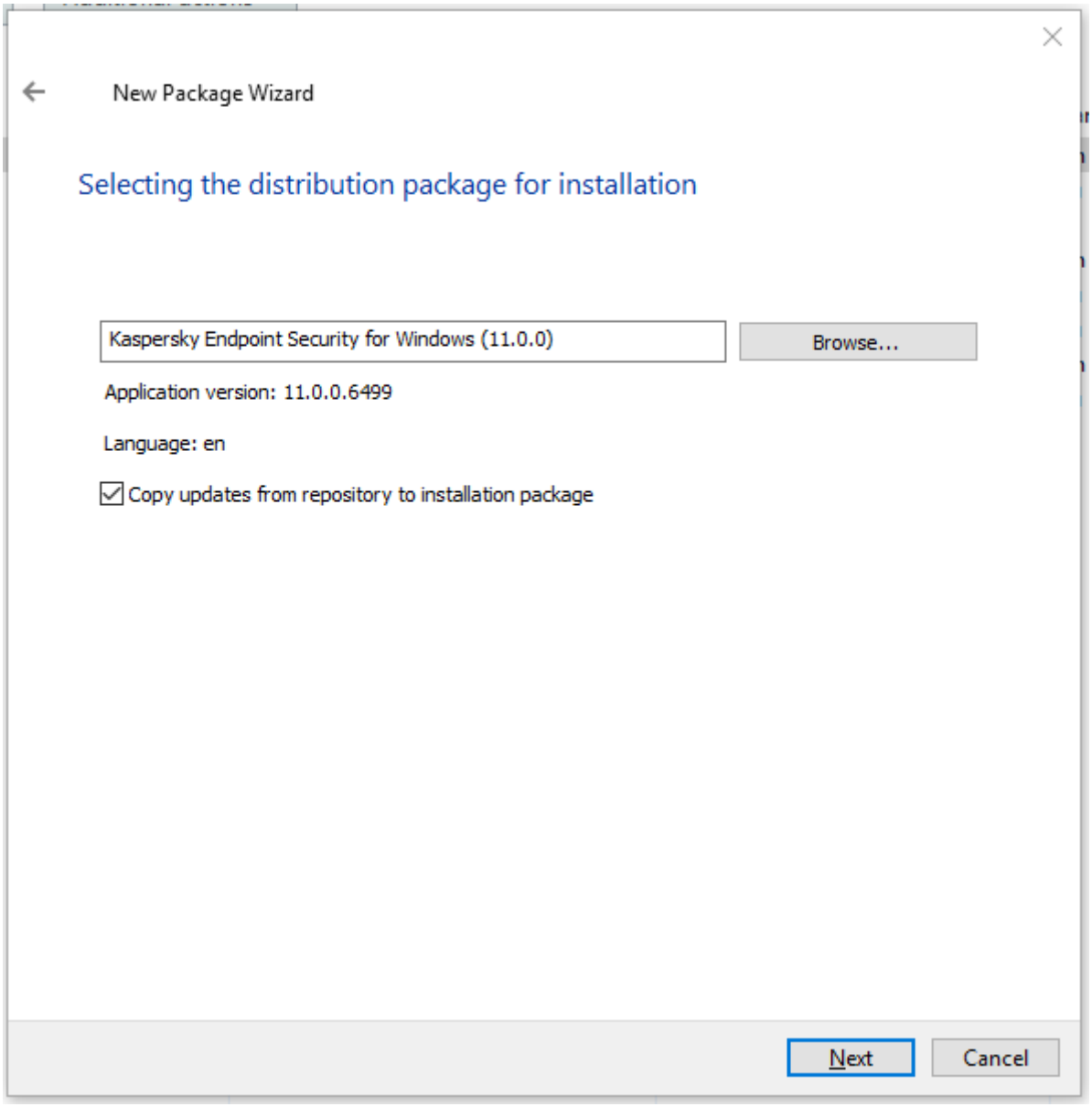
Navigate to Installation packages menu of KSC and choose “Create Installation package”. Wizard will start.



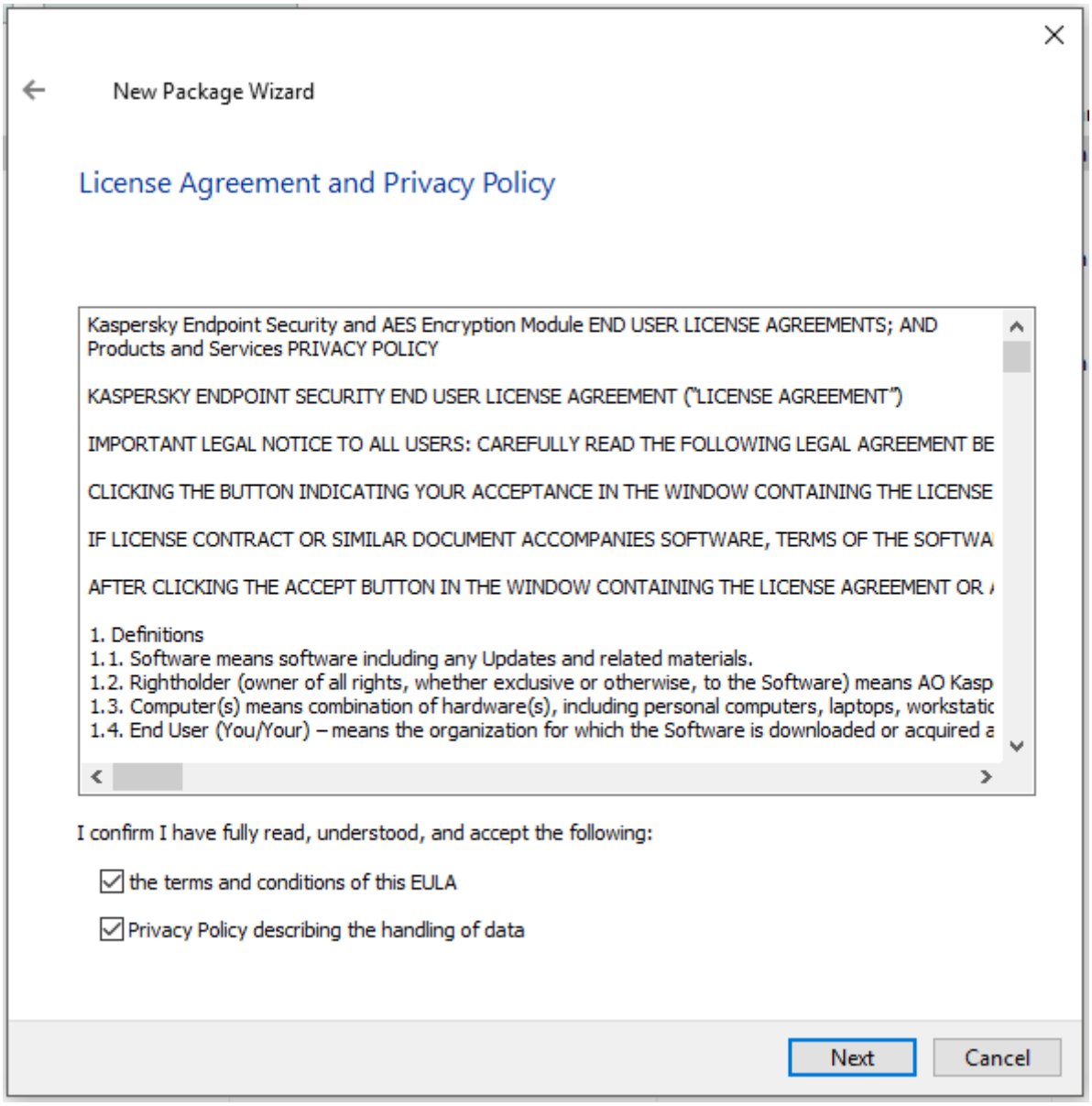
Select the installation package kes10winsp2_en_aes256.exe and wizard will import it.


New Package Wizard
Selecting the distribution package for installation
Browse...
Extracting
Self-extracting Kaspersky Lab application installation package is unpacking to temporary folder "kl_0a632315-7da4-4ca0-8fec-70b1f7dfebb3".
Please wait...
Next
Cancel

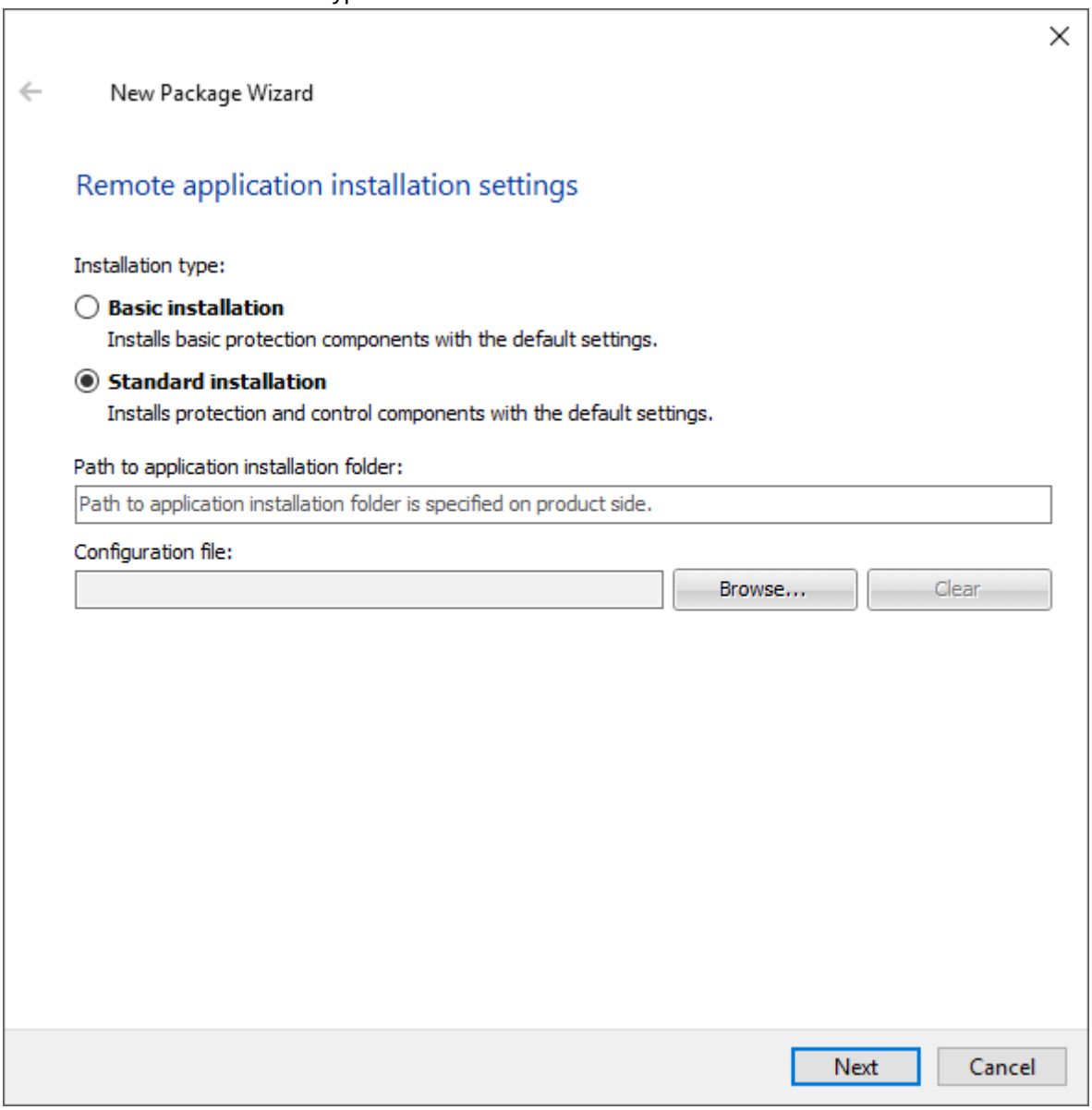
Uncheck “Copy Updates” checkbox.

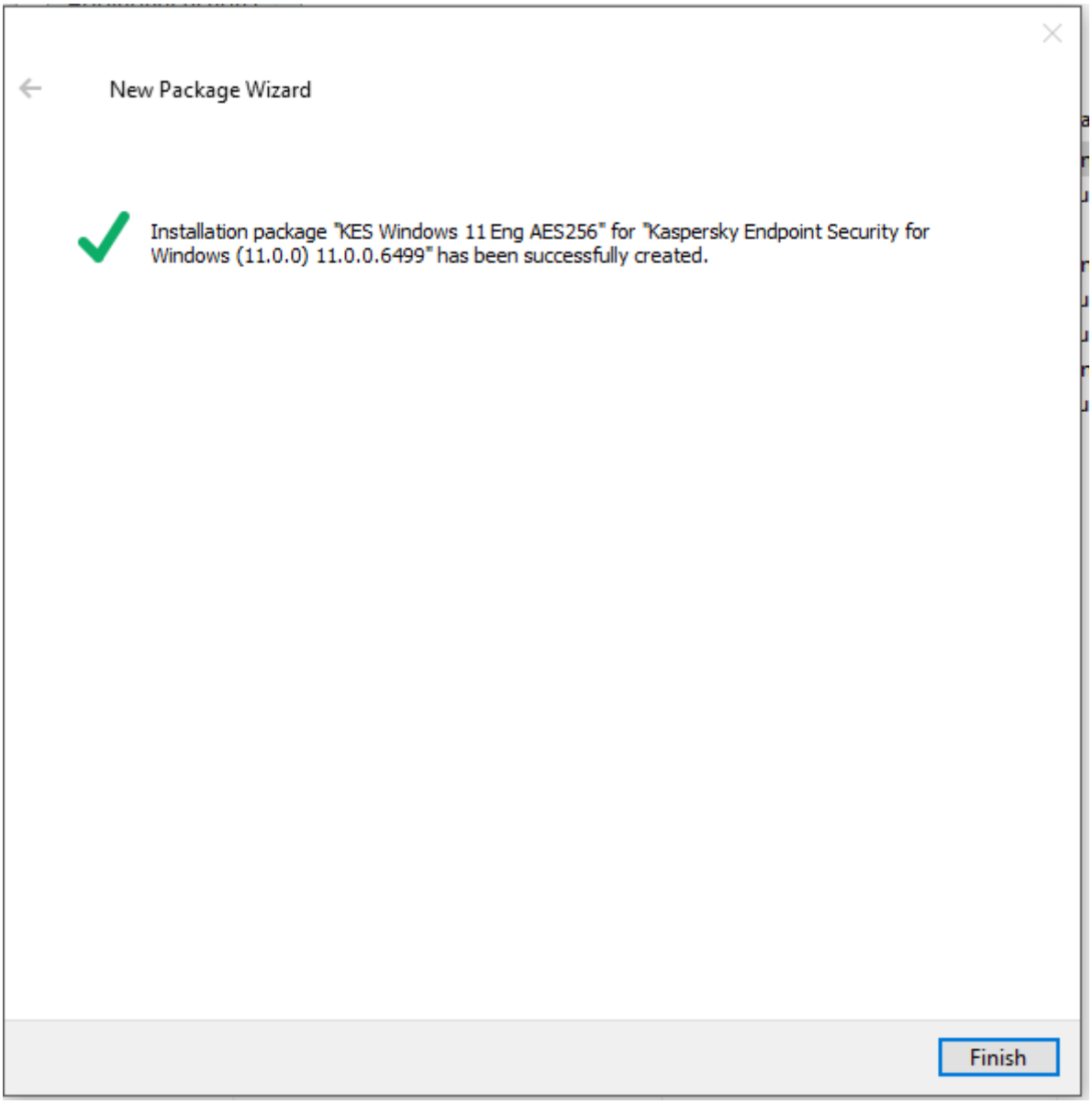


Accept the EULA.



Choose Standard installation type.

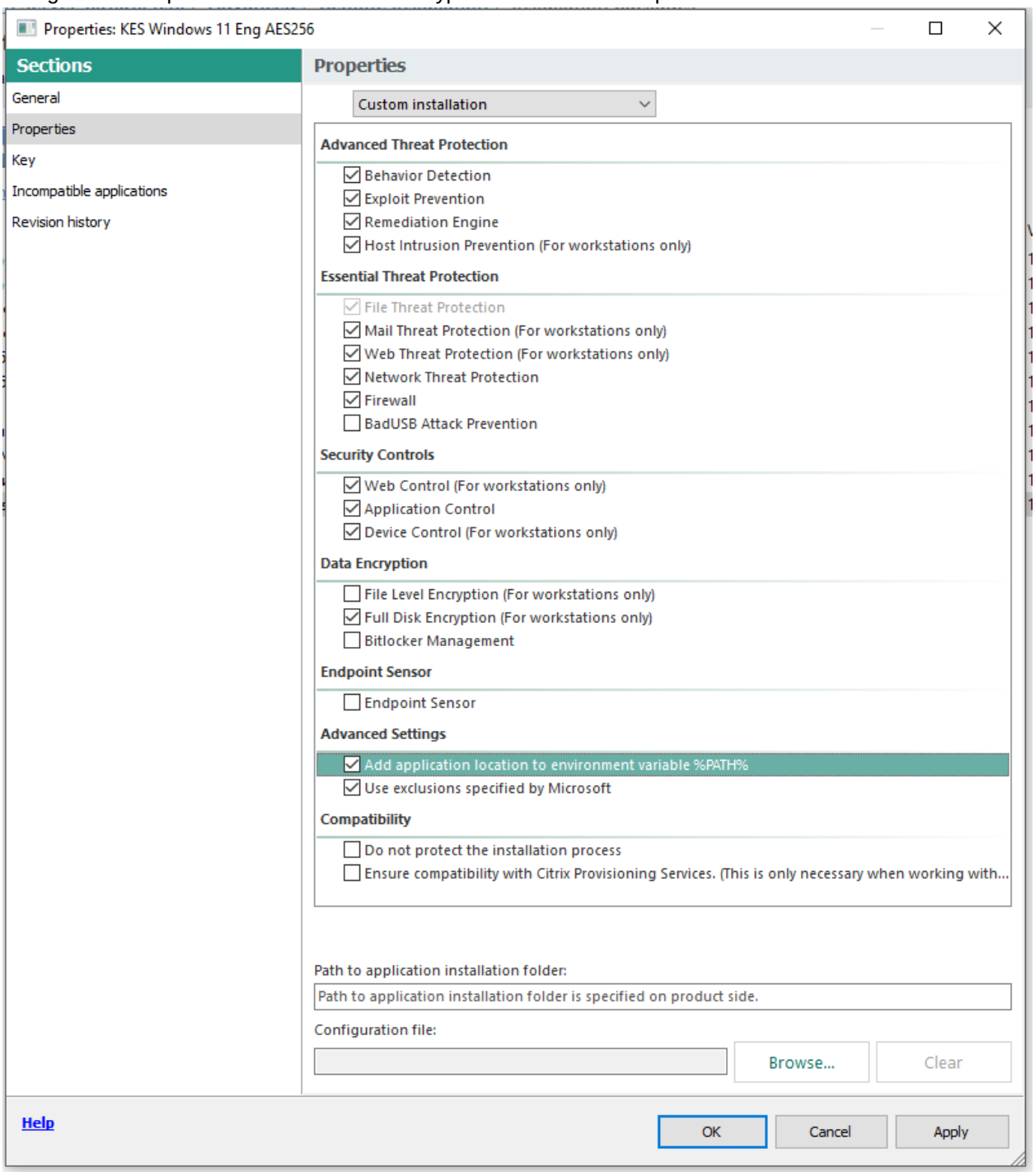




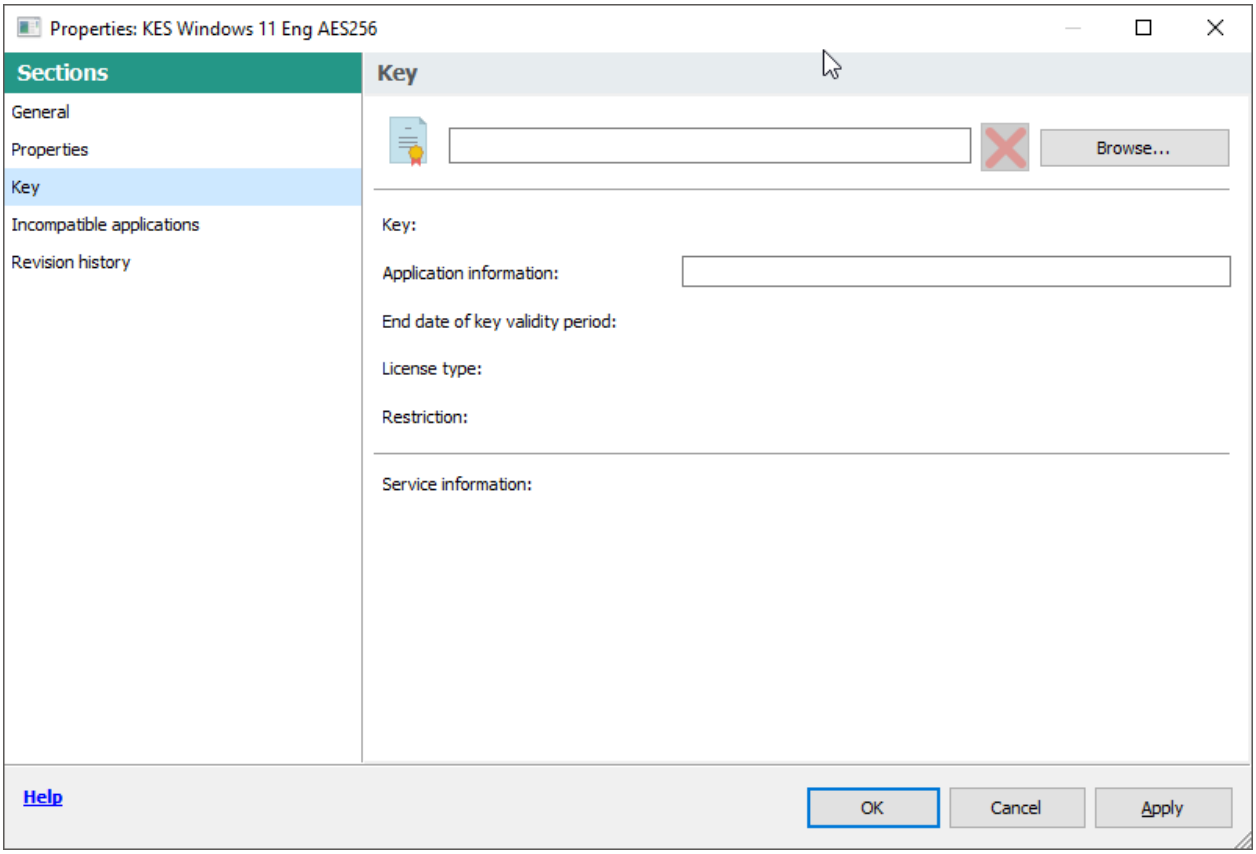
Wizard finishes.

Navigate to “Installation packages” windows. Select the package and click Configure Installation package.

Navigate to Components list and check Encryption for Hard Drive option.



You may also include Activation key into instalation package.



After you created a package, in the console tree, open the **Remote installation** folder and click **Deploy installation package on managed devices (workstations)** to run the Protection Deployment Wizard.

- In the **Select installation package** window of the Wizard specify the installation package of an application that you want to install.
- Follow the instructions of the Wizard.

The Wizard's activities create a remote installation task to install the application to client computers. You can start or stop the task in the **Tasks** folder.

Preparative procedures.

Annex 3. Installing KSC Network Agent

Network Agent can be installed in non-interactive mode, i.e., without interactive input of installation settings. This requires an installation MSI package of Network Agent located in the distribution package of Kaspersky Security Center, in the folder Packages\NetAgent\exec.

To install Network Agent on a local device in non-interactive mode, run the command

```
msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
```

where setup_parameters is a list of settings and their respective values separated by a space (PRO1=PROP1VAL PROP2=PROP2VAL).

Names and possible values of settings that can be used when installing Network Agent in non-interactive mode are listed in the table below.

Settings of Network Agent installation in non-interactive mode

INSTALLDIR	Path to the Network Agent installation folder	String value
SERVERADDRESS	Administration Server address	String value
SERVERPORT	Port number to connect to Administration Server.	Numerical value
SERVERSSLPORT	Port number to connect to Administration Server by using SSL protocol.	Numerical value
USESSL	Whether to use SSL connection	• 1 – Use • Other value or no value – Do not use
OPENUDPPORT	Whether to open a UDP port	• 1 – Open • Other value or no value – Do not open
UDPPORT	UDP port number	Numerical value
USEPROXY	Whether to use a proxy server	• 1 – Use • Other value or no value – Do not use
PROXYADDRESS	Proxy address	String value
PROXYPORT	Number of port for connection to Administration Server	Numerical value
PROXYLOGIN	Name of an account for connection to a proxy server	String value
PROXYPASSWORD	Password of account for connection to proxy server. Do not specify any details of privileged user accounts in the settings of installation packages.	String value
GATEWAYMODE	Connection gateway use mode:	• 0—Do not use connection gateway. • 1—Use as connection gateway the device on which Network Agent is to be installed. • 2—Connect to the Administration Server

		via another connection gateway.
GATEWAYADDRESS	Connection gateway address	String value
CERTSELECTION	Method of receiving a certificate	• GetOnFirstConnection – Receive an Administration Server certificate • GetExistent – Select an existing certificate
CERTFILE	Path to the certificate file	String value
VMVDI	Whether to enable the dynamic mode for VDI	• 1 – Enable • Other value or no value – Do not enable
LAUNCHPROGRAM	Whether to run the Network Agent service after installation completion	• 1 – Run • Other value or no value – Do not ru

In order to satisfy security opbjectives USESSL parameter should be set to 1.