

kaspersky

Kaspersky Endpoint Security for Windows

(version 11.6.0.394 AES256)

Preparative Procedures

Document version: 2.03

26.11.2021

Table of Contents

- 1 About this document.....4
 - 1.1 Terminology4
 - 1.2 References.....4
- 2 Introduction.....5
 - 2.1 ST Reference.....5
 - 2.2 Product Reference5
 - 2.3 Requirements and prerequisites.....5
 - 2.3.1 Hardware5
 - 2.3.2 Software.....5
 - 2.3.3 KSC management software5
- 3 Security Objectives.....6
 - 3.1 KSC management6
 - 3.2 TOE secure operation.....6
 - 3.3 Trusted administration6
 - 3.4 Correct behaviour of authorised users6
- 4 Preparative procedures7
 - 4.1 OS setup7
 - 4.1.1 Secure Boot has to be enabled on supported systems7
 - 4.1.2 Safe mode boot for OS is disabled7
 - 4.2 Check installation package7
 - 4.3 Kaspersky Security Center (KSC)7
 - 4.3.1 KSC installation.....7
 - 4.3.2 KSC settings7
 - 4.3.3 Set up KSC connection.....8
 - 4.3.4 Install management plug-in.....8
 - 4.4 Product Installation8
 - 4.4.1 Manual installation8
 - 4.4.2 Remote installation9
 - 4.4.3 Install activation keys9
 - 4.4.4 Upgrade from previous version.....9
 - 4.5 Set up policies for Kaspersky Endpoint Security for Windows9
 - 4.5.1 Setup settings password protection9
 - 4.5.2 Create encryption policy9
 - 4.5.3 Disable local Tasks11
 - 4.6 Configure organization-specific settings.....11
 - 4.6.1 Create relevant access policies11
 - 4.6.2 Create AV settings12
 - 4.6.3 Group tasks.....12
 - 4.7 Apply policies for Kaspersky Endpoint Security for Windows12

4.7.1	Apply created policy	12
4.7.2	Verify that encryption tasks are finished on endpoint machines	13
4.8	Create tasks for managed computer running Kaspersky Endpoint Security for Windows	16
4.8.1	Create group tasks.....	16
4.8.2	Modify existing Update task to disable AV updates.....	16
Annex 1.	Installation walkthrough	18
Annex 2.	Remote Installation.....	23
Annex 3.	Installing KSC Network Agent	28

1 About this document

1.1 Terminology

Terms and acronyms, most of them specific to Kaspersky 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
TLS	Communication secured by Transport Layer Security Protocol v.1.2.
TOE	Target of Evaluation (Kaspersky Endpoint Security for Windows)

1.2 References

Reference	Document
[ST]	Kaspersky Endpoint Security for Windows. Security Target. Version 2.04
[UGD]	Kaspersky Endpoint Security for Windows. User Manual. Version 2.01

2 Introduction

This document describes necessary preparative procedures for putting **Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)** into the evaluated secure state as required by [ST].

2.1 ST Reference

Kaspersky Endpoint Security for Windows. Security Target. Version 2.04.

2.2 Product Reference

Described product is the **Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256)** developed by AO Kaspersky Lab.

2.3 Requirements and prerequisites

2.3.1 Hardware

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

- 2 GB free disk space on the hard drive
- CPU:
 - Workstation: 1 GHz
 - Server: 1.4 GHz
 - Support for the SSE2 instruction set
- RAM:
 - Workstation (x86): 1 GB
 - Workstation (x64): 2 GB
 - Server: 2 GB
- Microsoft .NET Framework 4.0 or later.
- Network connection peripherals.

2.3.2 Software

Kaspersky Full Disk Encryption is available only for computers running a Windows operating system for workstations:

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 or later;
- Windows 8 Professional / Enterprise;
- Windows 8.1 Professional / Enterprise;
- Windows 10 Home / Pro / Education / Enterprise.

For computers running a Windows operating system for servers, use BitLocker Drive Encryption technology.

Kaspersky Endpoint Security supports full disk encryption in FAT32, NTFS and exFat file systems only.

Be aware of all Encryption functionality limitations: <https://support.kaspersky.com/KESWin/11.6.0/en-US/130984.htm>

2.3.3 KSC management software

Kaspersky Security Center 13 has to be installed. You may obtain KSC installation package and documentation from the Kaspersky website: <https://www.kaspersky.com/small-to-medium-business-security/downloads/security-center>

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 the 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 TLS connection that is provided by the environment. The Network Agent of the KES has to be used. The Network Agent's TLS 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 the 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

Refer to the device manual for instructions.

4.1.2 Safe mode boot for OS is disabled

Refer to the OS documentation for instructions.

4.2 Check installation package

Download an installation package from Kaspersky Lab support website (<https://support.kaspersky.ru/15736>).

Compare checksums of the TOE with ones listed in [ST] to make sure you are using the certified package.

You may use tools of your choice that support calculation of SHA256 hash or CertUtil tool included into MS Windows installation. In latter case you should use following command:

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

Compare the calculated checksum to the one listed in [ST] and/or published on the Kaspersky Lab website.

4.3 Kaspersky Security Center (KSC)

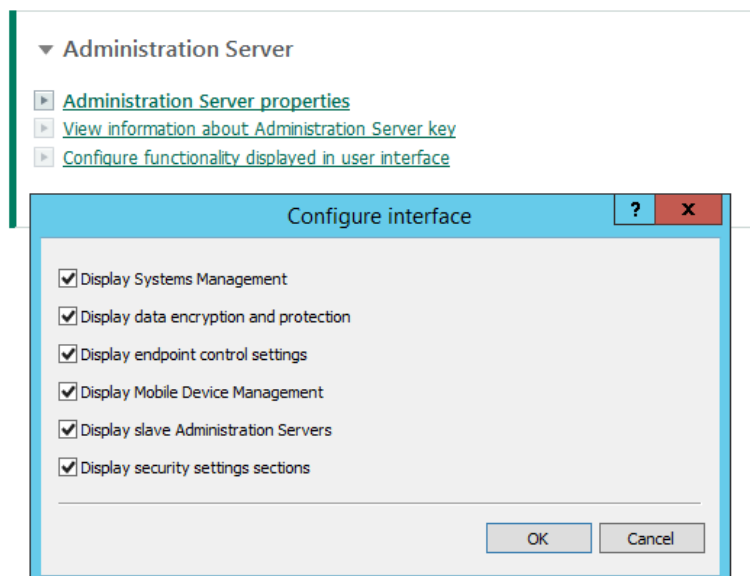
You can use Kaspersky Security Center for centralised deployment of KES in your local network.

4.3.1 KSC installation

Make sure Kaspersky Security Center 13 is installed in secure environment as per 3.1 and configured in secure manner.

4.3.2 KSC settings

Use the following settings in the 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 KES, and set up the connection to KSC.

Make sure connection is secured using TLS. The Network Agent will download a KSC digital certificate at first connection, or you can provide it manually. Refer to Annex 3 of this document for details.

Check that all machines have “Network Agent is installed” mark shown in KSC interface (Devices > Managed Devices).

4.3.4 Install management plug-in

On the device with MMC-based Console installed, run the klcfinst.exe file, which is included in the KES distribution package.

In order to install a management plug-in for Web Console refer to “Installing the web plug-in” section of [UGD].

4.4 Product Installation

4.4.1 Manual installation

You may install the product 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.

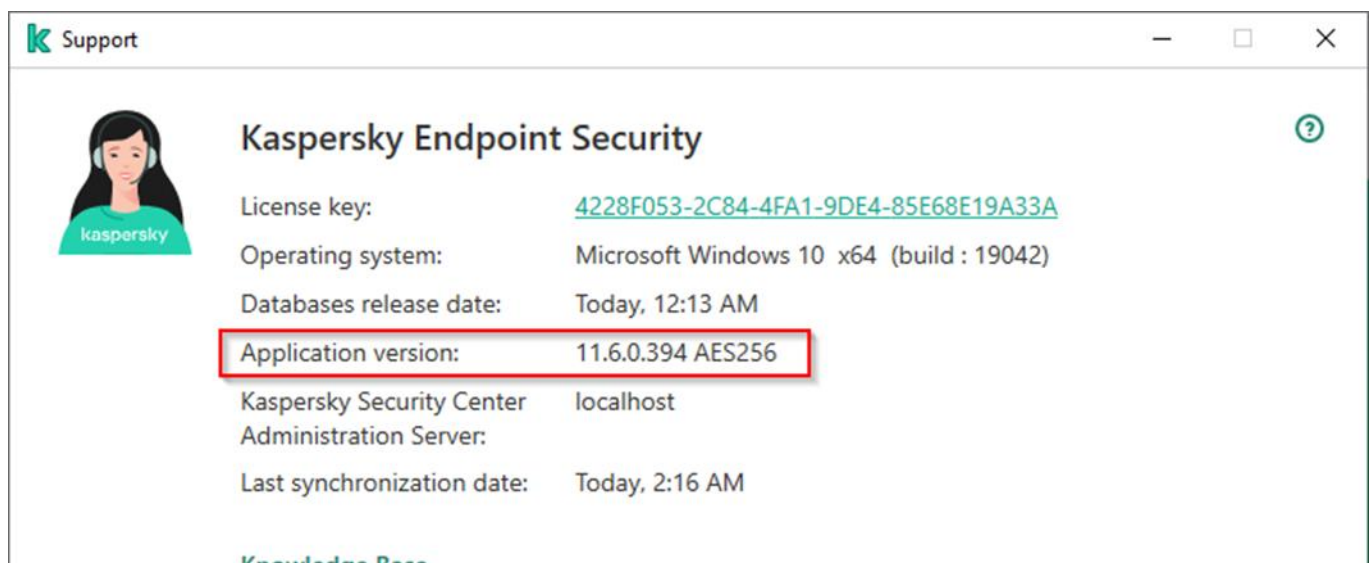
Make sure “Full Disk Encryption” option is checked.

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 the version of the installed product

Use Support button () in the GUI to verify the Application version is **11.6.0.394 AES256** as shown in screenshot below.



The screenshot shows a window titled "Support" with a Kaspersky logo. It displays the following information for "Kaspersky Endpoint Security":

License key:	4228F053-2C84-4FA1-9DE4-85E68E19A33A
Operating system:	Microsoft Windows 10 x64 (build : 19042)
Databases release date:	Today, 12:13 AM
Application version:	11.6.0.394 AES256
Kaspersky Security Center Administration Server:	localhost
Last synchronization date:	Today, 2:16 AM

At the bottom, there is a "Knowledge Base" link.

4.4.2 Remote installation

You may install the product 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 4.4.1.3 or via KSC's Report on Kaspersky software versions.

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 “Activating the application through Kaspersky Security Center” section of [UGD] for instructions on how to import and rollout activation keys. Imported keys should be able to activate KES 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 for Windows of previous versions to version 11.6.0.394 AES256 by installing the product as described above. Previous version will be automatically removed and replaced by new product version.

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

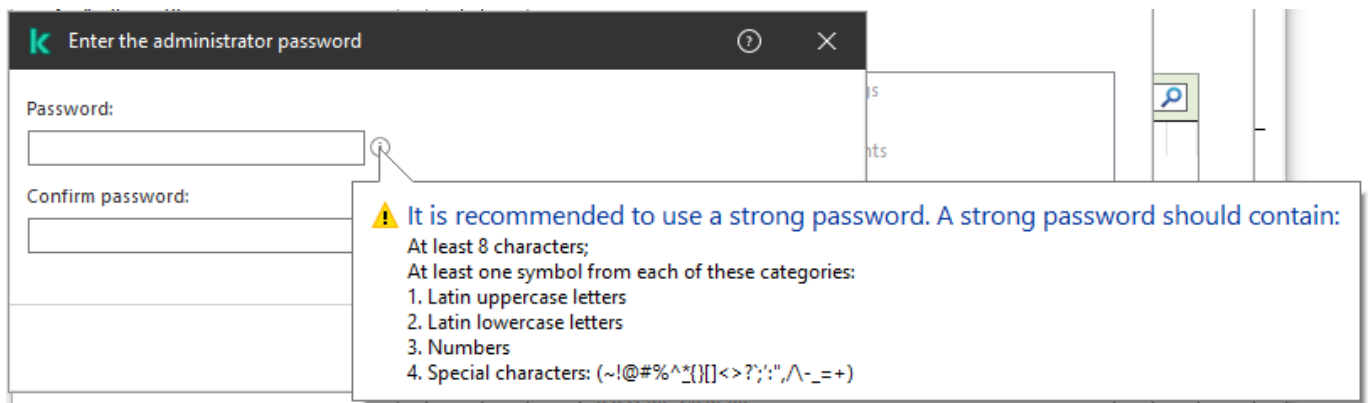
4.5 Set up policies for Kaspersky Endpoint Security for Windows

Refer to “Managing policies” section in [UGD] for help when creating policies for Kaspersky Endpoint Security for Windows in KSC.

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

4.5.1 Setup settings password protection

Refer to “Password protection” section in [UGD]. 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 8+ length.



4.5.2 Create encryption policy

Refer to “Data Encryption” section in [UGD] for more details and explanation of this.

4.5.2.1 Policy should have Single Sign-On feature disabled

Refer to “Enabling Single Sign-On (SSO) technology” section in [UGD].

Password settings

Configure passwords for Authentication Agent

Block password after

5

failed input attempt(s) (1-20)

Use Single Sign-On (SSO) technology

Minimum password length (1-50 characters)

8

Change password after

30

days of use (1-365)

Assess password strength

Capitals must be used

Digits must be used

Special characters must be used: !,;, "N%&

Block reuse of a previous password

Prompt for password change on the first system logon

4.5.2.2 Policy should cover all hard disk

Encryption settings

Encryption mode

Encrypt all hard drives

During encryption, automatically create Authentication Agent accounts for Windows users

4.5.2.3 Encryption task should create accounts for users

Encryption settings

Encryption mode

Encrypt all hard drives

During encryption, automatically create Authentication Agent accounts for Windows users

[Authentication Agent account creation settings](#)

- Automatically create Authentication Agent accounts for all users of this computer upon sign-in
- Save user name entered in Authentication Agent
- Encrypt used disk space only (reduces encryption time)
This function cannot be enabled or disabled after encryption starts. It is recommended to use this function for new, unused devices. If a device already has any data stored on it, it is recommended to encrypt the entire drive to protect all data.
- Use Legacy USB Support (not recommended)

[Exclusions](#)

Password settings

Configure passwords for Authentication Agent

Block password after

5

failed input attempt(s) (1-20)

Use Single Sign-On (SSO) technology

Minimum password length (1-50 characters)

8

Change password after

30

days of use (1-365)

- Assess password strength
 - Capitals must be used
 - Digits must be used
 - Special characters must be used: !,;,?N#%
- Block reuse of a previous password
- Prompt for password change on the first system logon

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.

Task management

Allow use of local tasks

Allow group tasks to be displayed

Allow management of group tasks

4.6 Configure organization-specific settings

You may modify the policy created in section 4.5 to meet your organizational rules and policies.

4.6.1 Create relevant access policies

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

Please be aware that Application Startup Control, Web Access Control, and Device Access Control must not be disabled in order to keep the evaluated secure state (certified configuration) of the TOE.

4.6.2 Create AV settings

Review and modify, if needed, the settings for AV functionality that meet your organizational security policies, including relevant actions or exclusions.

4.6.3 Group tasks

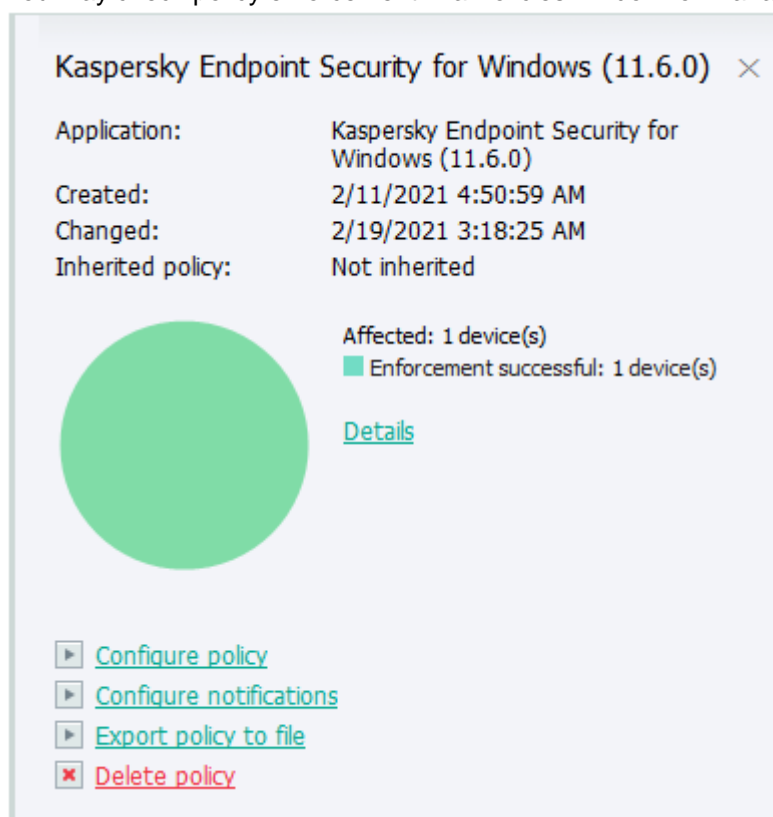
Create group tasks for different AV scans that users will be able to execute manually.

4.7 Apply policies for Kaspersky Endpoint Security for Windows

4.7.1 Apply created policy

You need to enforce the 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.



Kaspersky Endpoint Security for Windows (11.6.0) ×

Application:	Kaspersky Endpoint Security for Windows (11.6.0)
Created:	2/11/2021 4:50:59 AM
Changed:	2/19/2021 3:18:25 AM
Inherited policy:	Not inherited

Affected: 1 device(s)
■ Enforcement successful: 1 device(s)

[Details](#)

- ▶ [Configure policy](#)
- ▶ [Configure notifications](#)
- ▶ [Export policy to file](#)
- ✖ [Delete policy](#)

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/restart target machines to conduct initial test of hardware compatibility.

The screenshot shows the Kaspersky Endpoint Security console interface. The 'PROTECTION' tab is selected in the left sidebar. The main area displays the 'Encryption' section with the following details:

Visible	Yes
Device status	Warning
Status description	Restart is required
Protection status	Running
Last full scan	09/17/2021 2:21:10 pm
Virus detected	0
Objects that have failed disinfection	0
Encryption	
Disk encryption status	Applying the policy restart is required

A red box highlights the text 'restart is required' in the 'Disk encryption status' row. Below this, there is a link: [View data encryption errors](#).

Authentication agent



Full disk encryption compatibility test.

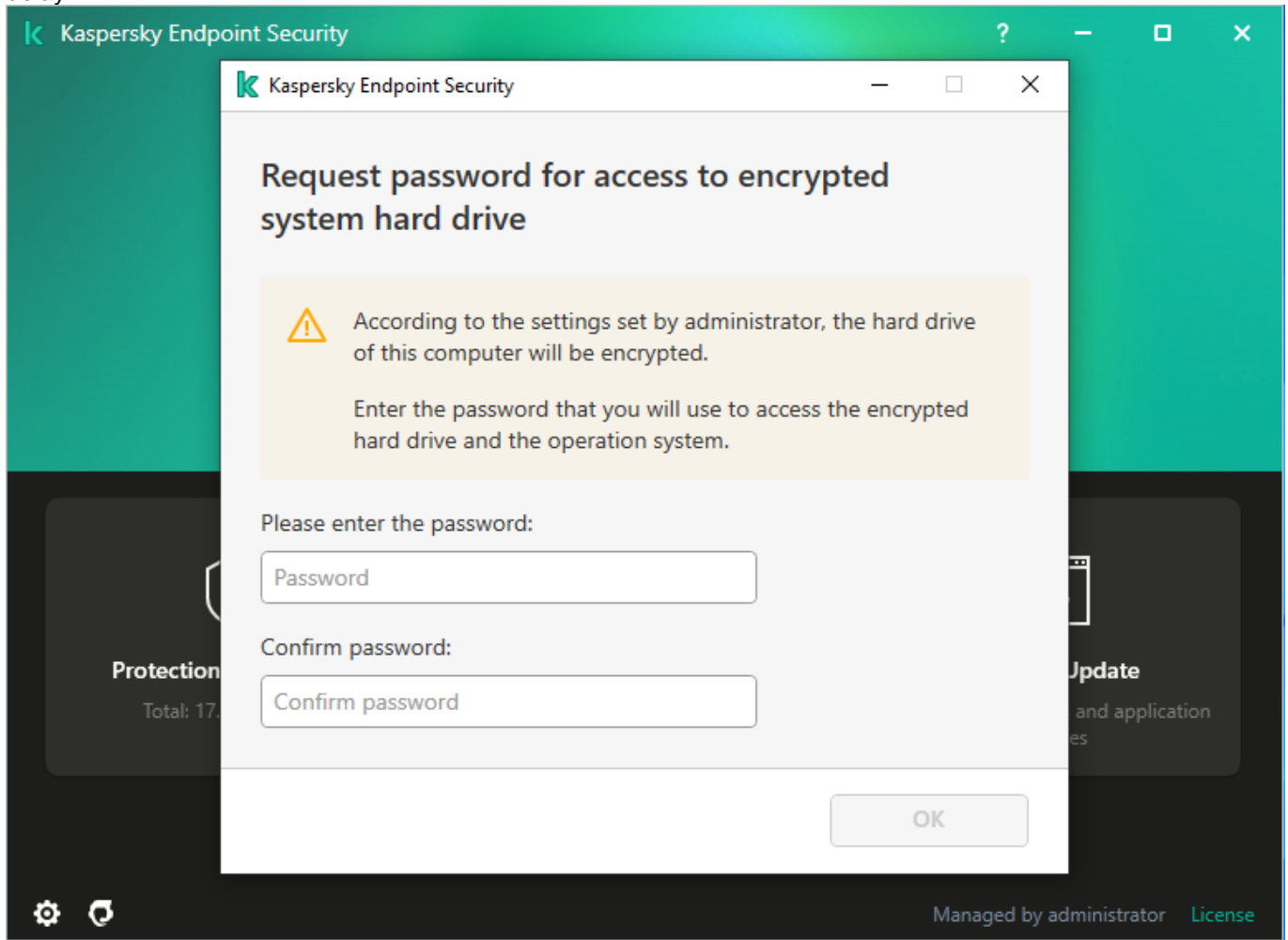
System administrator has applied full disk encryption policy on your computer. On this reboot we are checking compatibility of hardware and firmware with preboot authentication agent.

Click Continue or press any key to start Windows.

CONTINUE

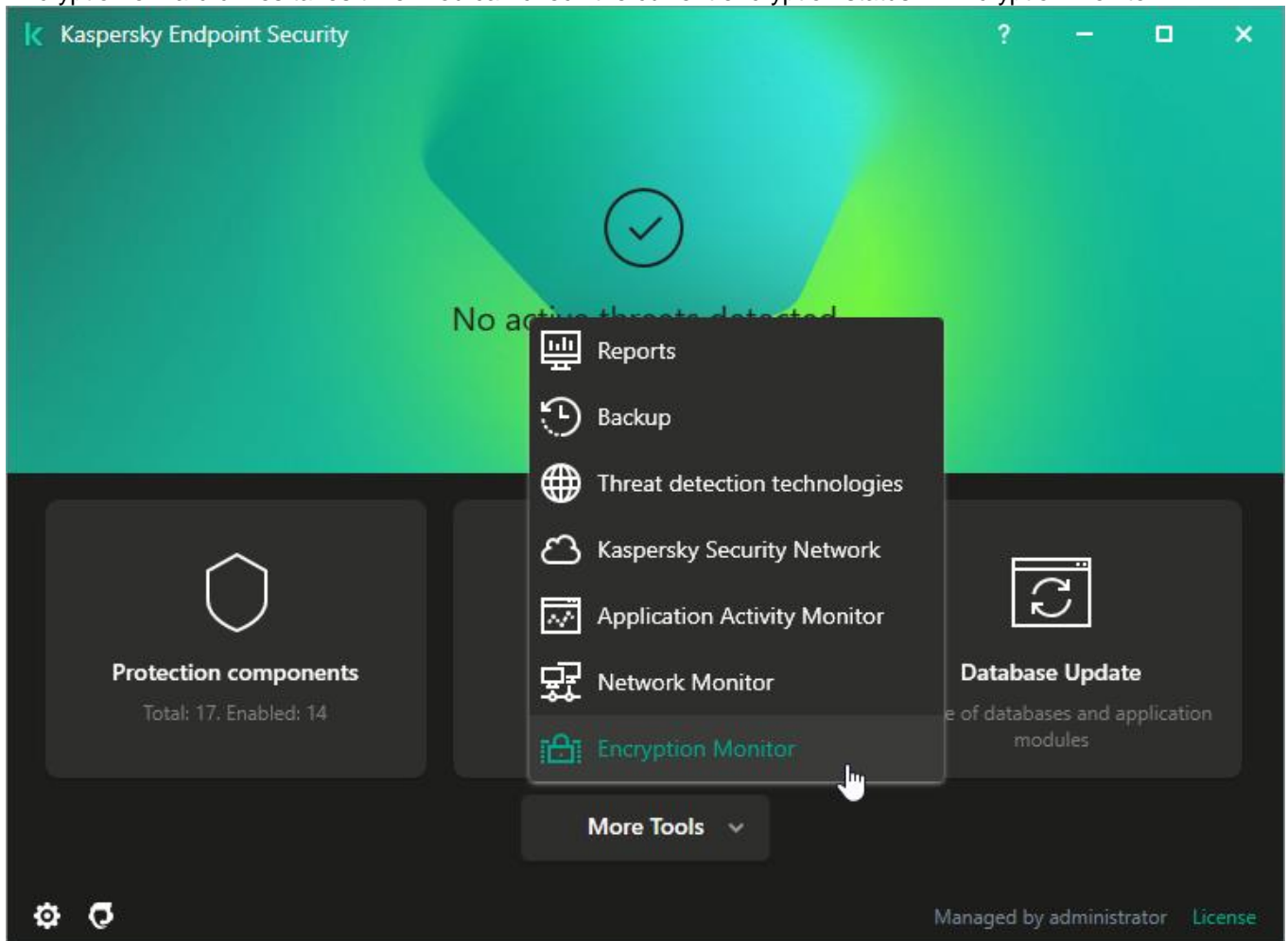
DESKTOP-Q9N1073

Users will then be prompted to enter password for encrypted drive. The prompt window may appear with a certain delay.



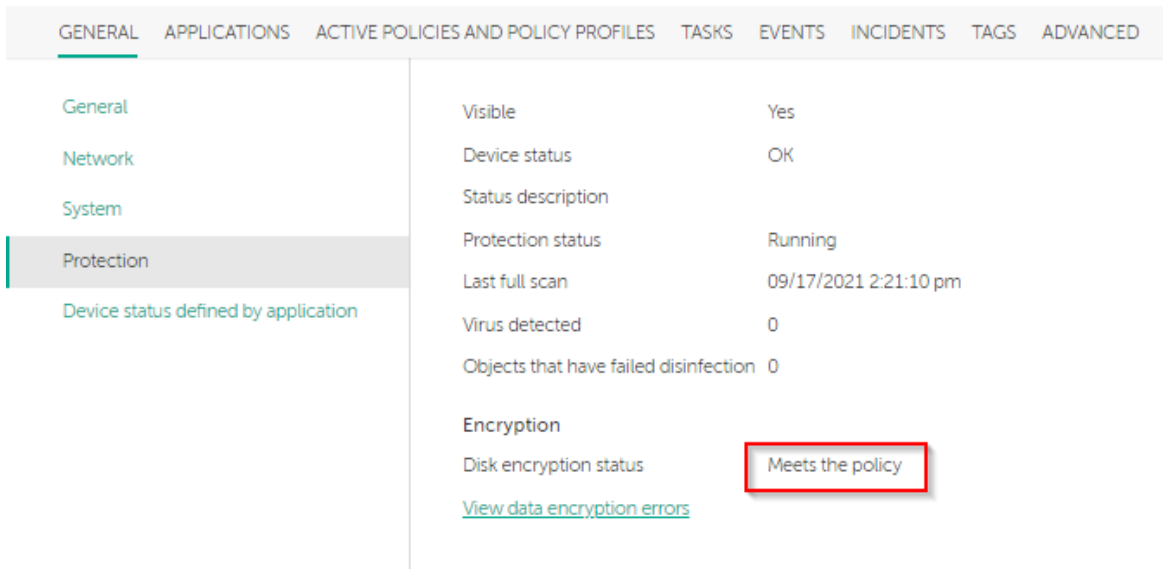
4.7.2.2 Status of encryption

Encryption of hard drives takes time. You can check the current encryption status in Encryption Monitor.



Encryption Monitor			
Encryption component	Object	Status	ID
Full Disk Encryption	Disk	encrypted for 100%	VMWare NVME_0000

You may also view encryption status of machine in KSC using Managed Devices properties. Disk encryption status should be “Meets the policy” (or “Complies with policy”, or “Compliant with policy”, which all have the same meaning).



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

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

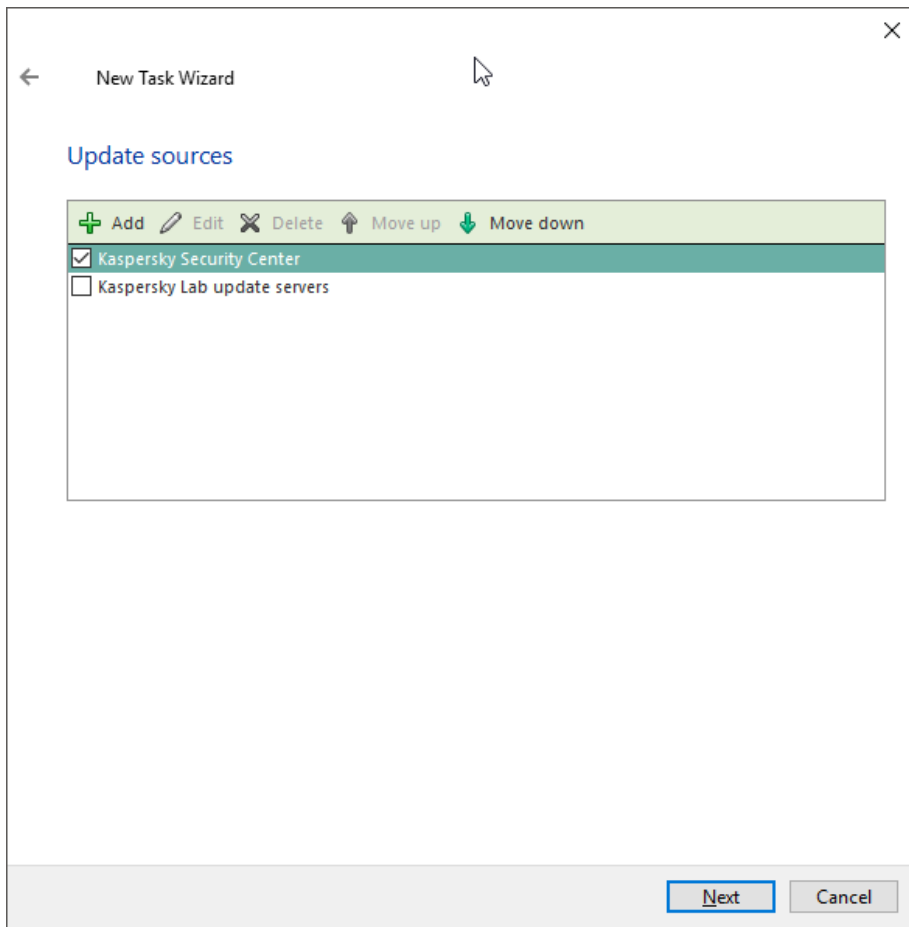
4.8.1 Create group tasks

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 updates¹

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

¹ As AV updates may include updated program modules that might affect product behaviour they are not allowed in the certified product state.

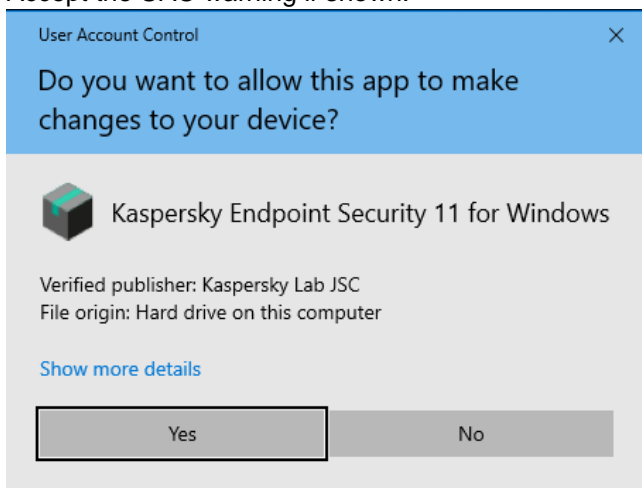


Annex 1. Installation walkthrough

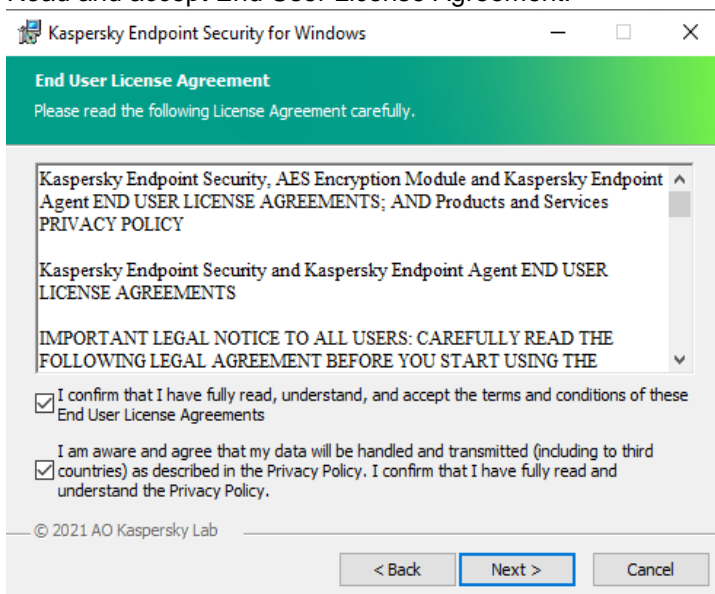
1. Unzip obtained package to created temporary directory.

Name	Date modified	Type	Size
agent	03.03.2021 13:22	File folder	
dotnet	03.03.2021 13:22	File folder	
bases.cab	05.02.2021 6:22	WinRAR archive	127 616 KB
cleaner.cab	05.02.2021 6:21	WinRAR archive	2 146 KB
incompatible.txt	05.02.2021 6:21	Text Document	66 KB
installer.ini	05.02.2021 6:21	Configuration setti...	1 KB
kes_win.kud	05.02.2021 6:21	KUD File	9 KB
kes_win.msi	05.02.2021 6:21	Windows Installer ...	126 264 KB
klcfginst.msi	05.02.2021 6:21	Windows Installer ...	21 812 KB
ksn_en.txt	05.02.2021 6:21	Text Document	33 KB
license.txt	05.02.2021 6:21	Text Document	79 KB
setup_kes.exe	05.02.2021 6:21	Application	660 KB

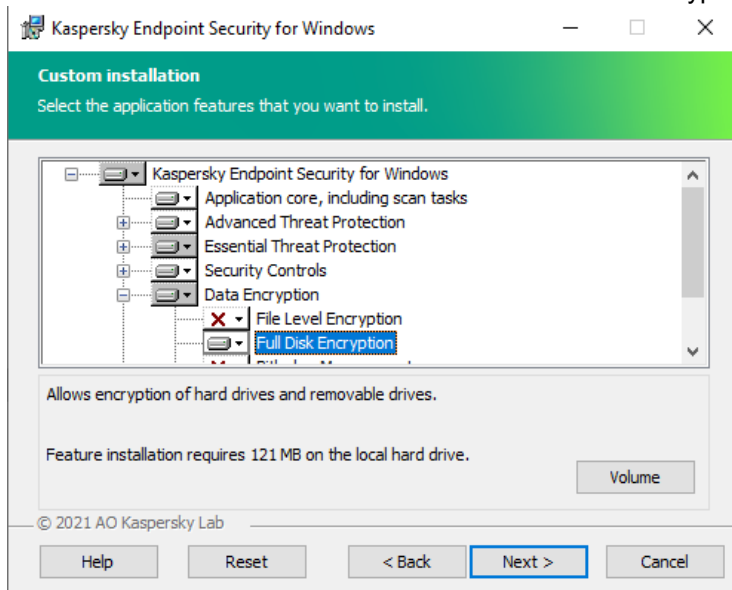
2. Navigate to the temporary folder created earlier and run `setup_kes.exe`.
3. Accept the UAC warning if shown.



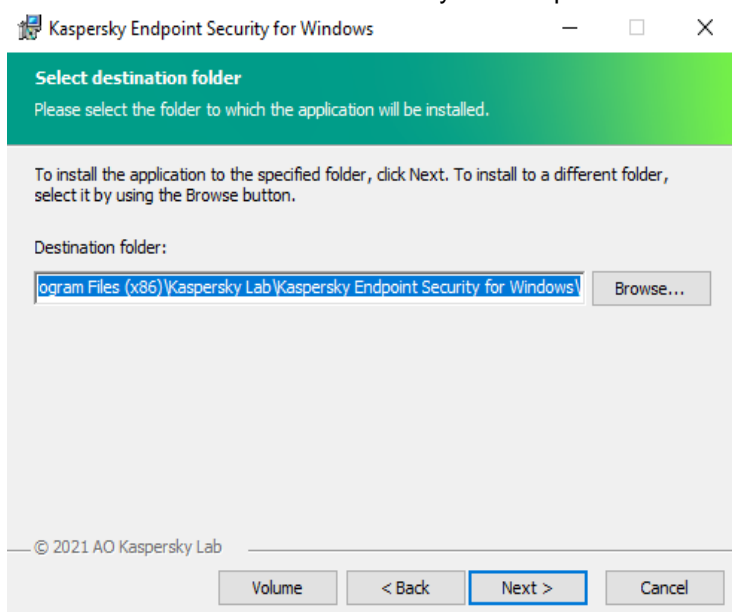
4. Setup will start.
5. Read and accept End User License Agreement.



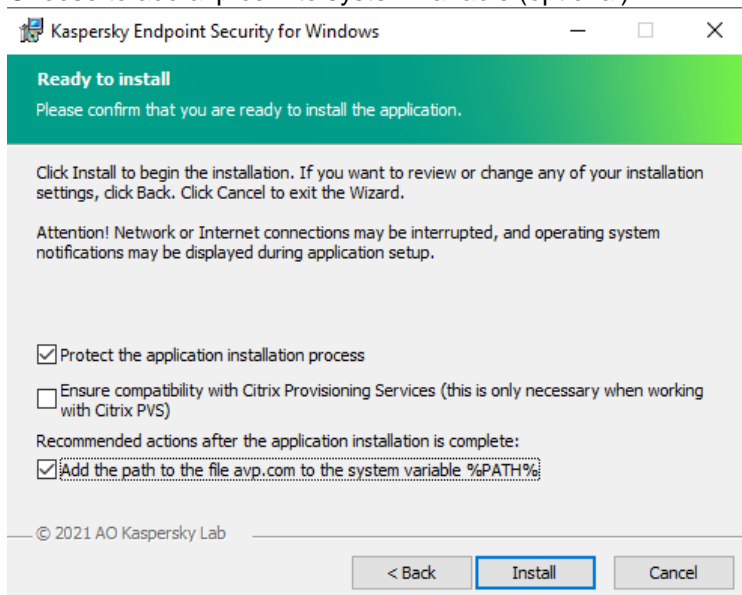
- In the next screen scroll down and choose “Full Disk Encryption” option to be installed.



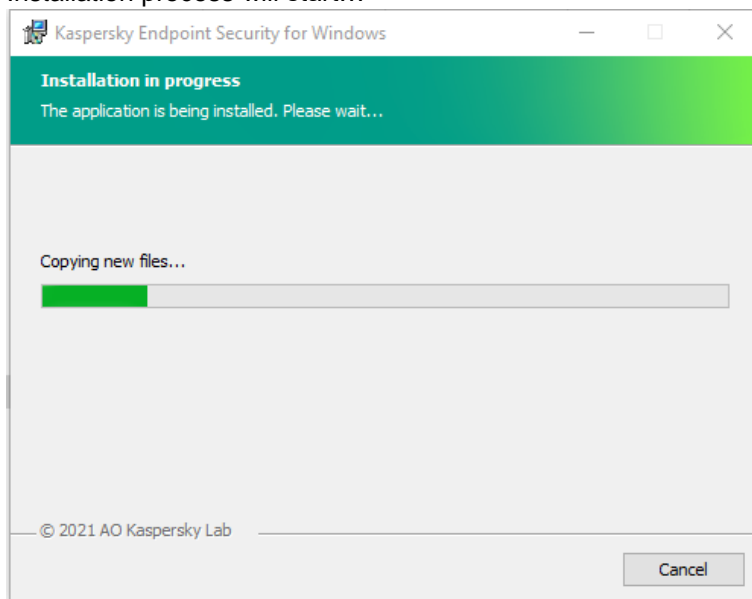
- Leave destination folder as offered by the setup.



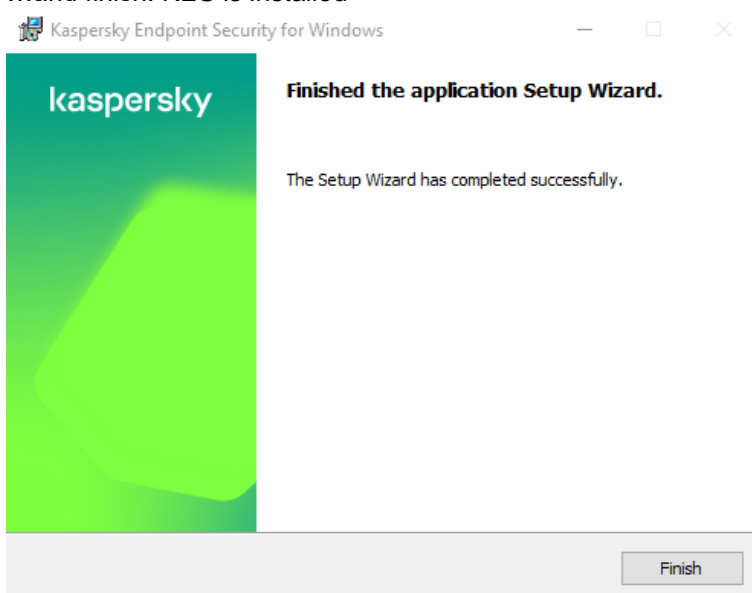
- Choose to add avp.com to system variable (optional).



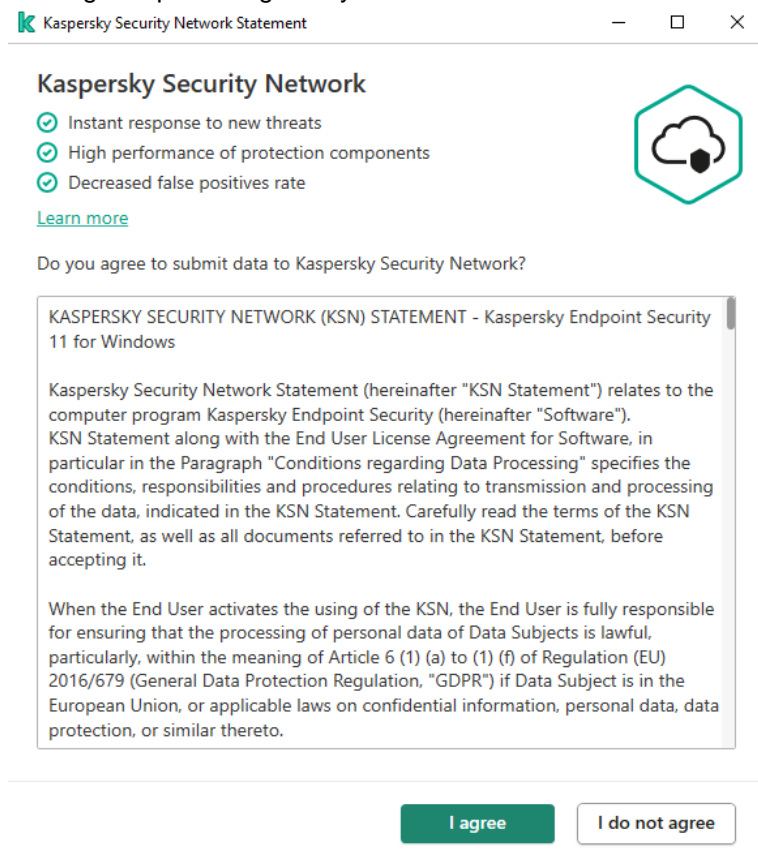
9. Installation process will start...



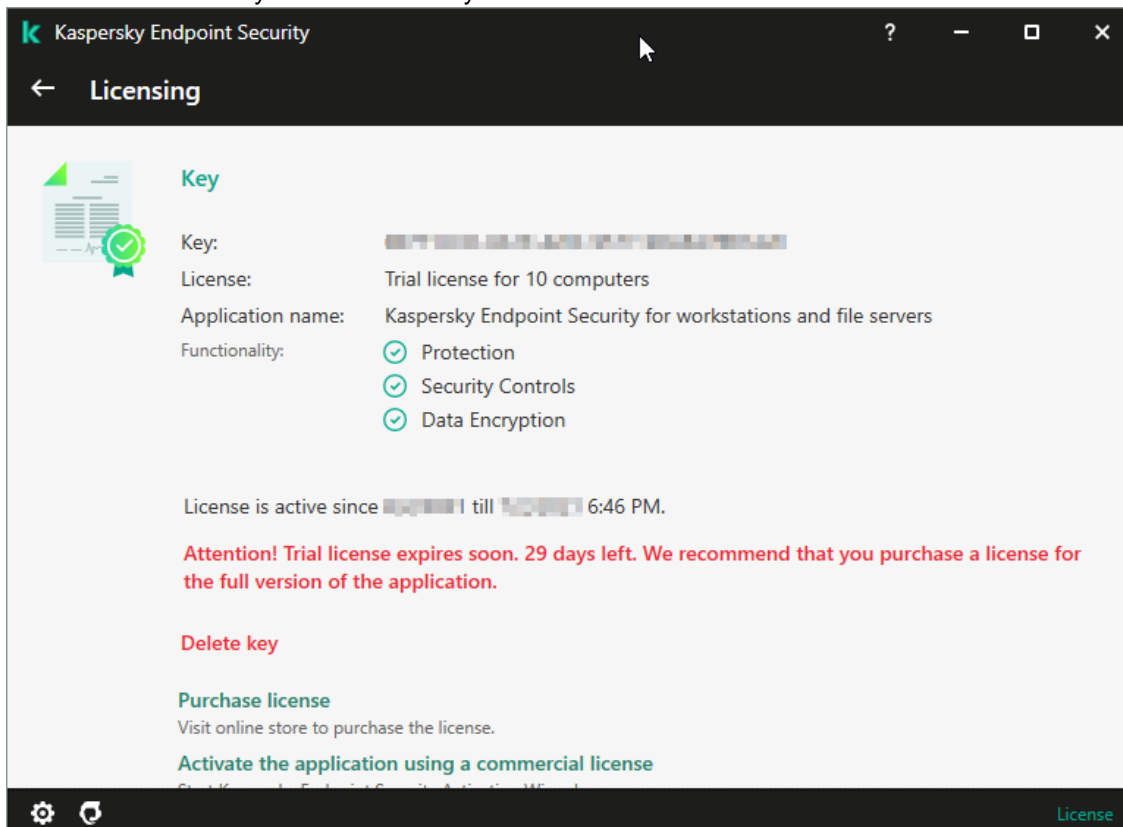
10. ...and finish. KES is installed



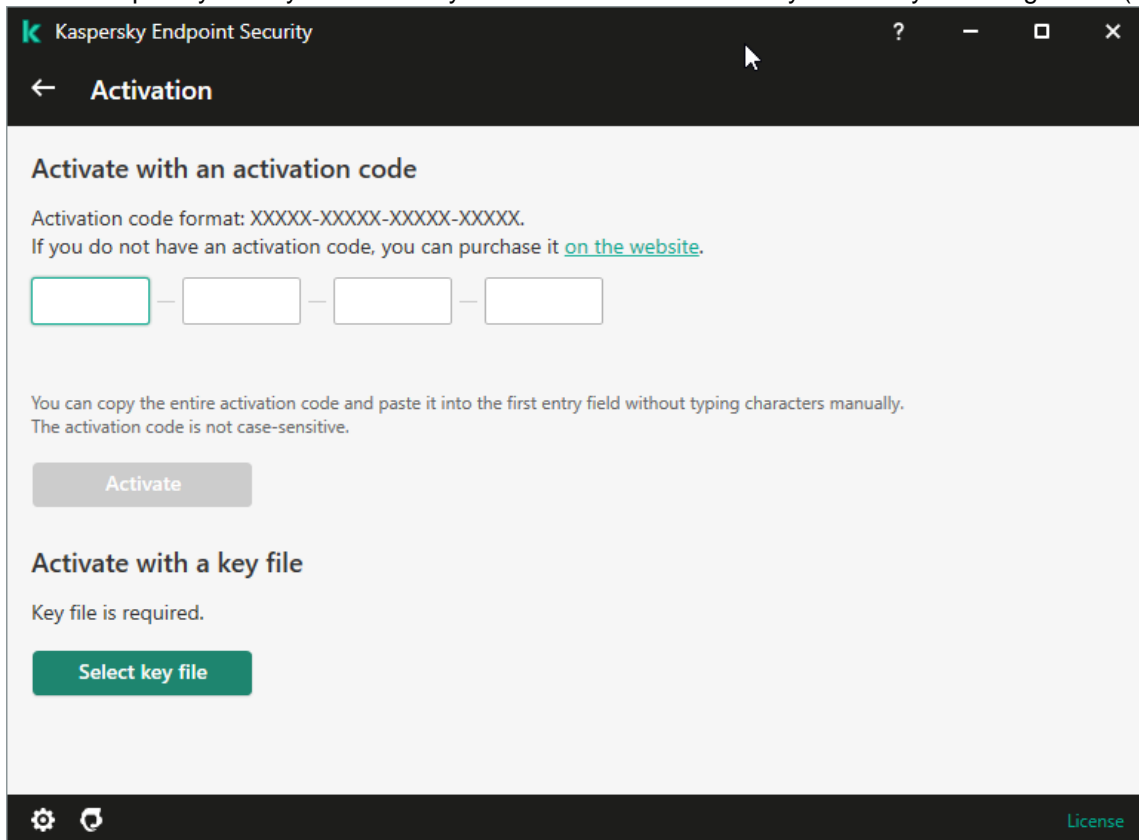
11. After you click Finish KES will be started and Kaspersky Security Network (KSN) Statement will be displayed. After you accept (or not accept) the agreement based on you company policies, KES will be running and protecting the system.



KES will automatically activate a 30 days trial version.



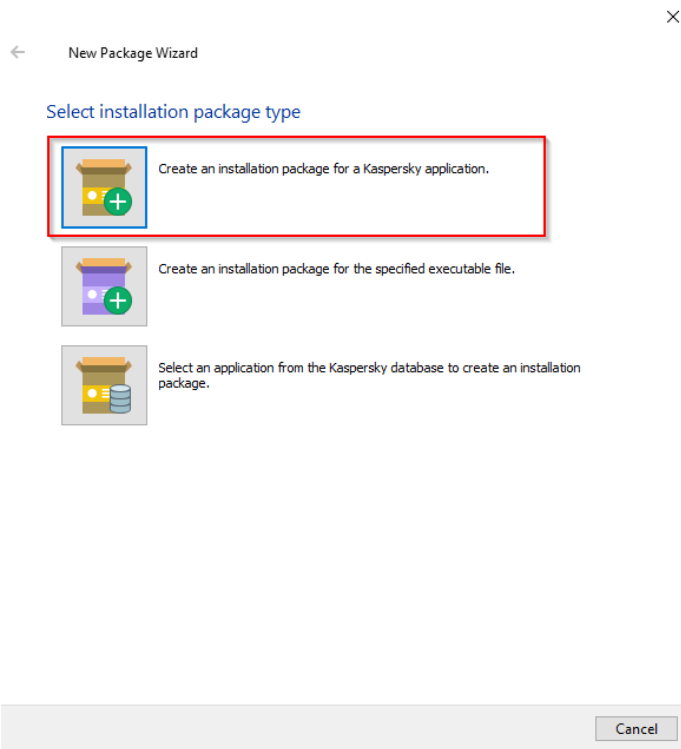
When it expires you may either enter your activation code / add key file locally or through KSC (see step 4.4.3).



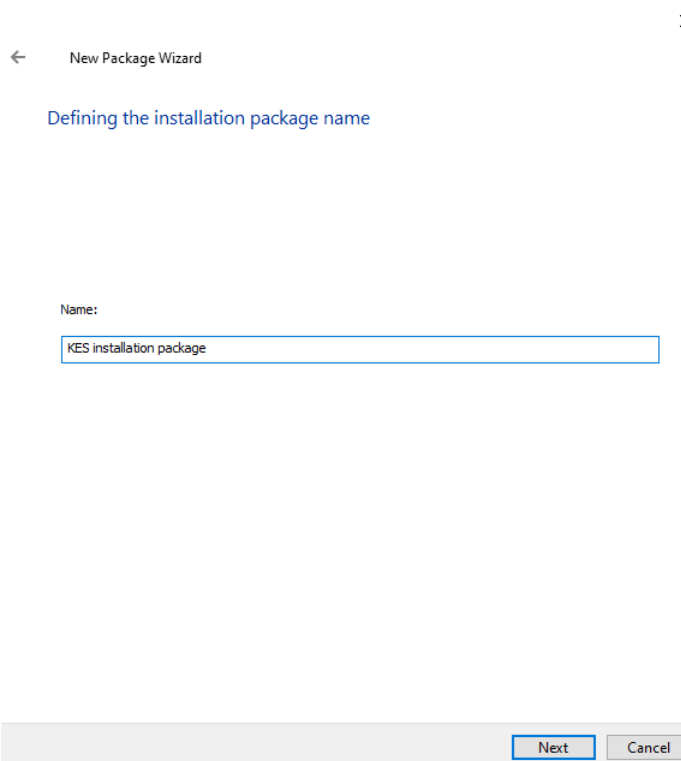
Annex 2. Remote Installation

Process is done in KSC MMC-based console.

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

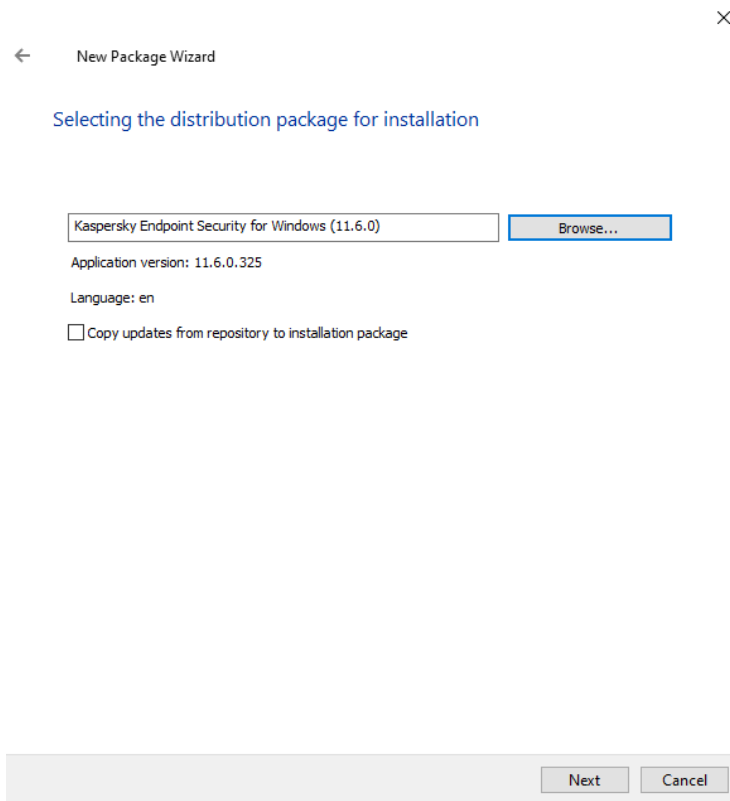


Select Create an installation package for a Kaspersky application.

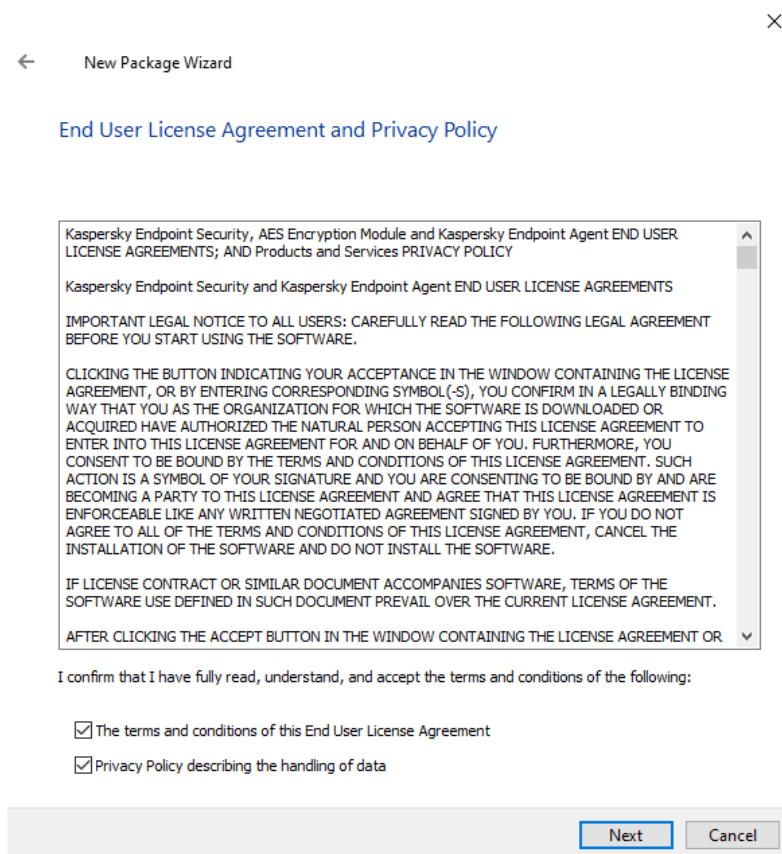


Name the package. Click Next.

Navigate to the folder where you have unpacked installation package and select kes_win.kud and wizard will import the package.



Uncheck “Copy updates from repository” checkbox. Click Next.



Accept the terms and conditions of EULA and Privacy Policy. Click Next.

← New Package Wizard ×

Uploading installation package to the Administration Server

Uploading package files to the Administration Server...



Next

Cancel

Wait until the package is created.

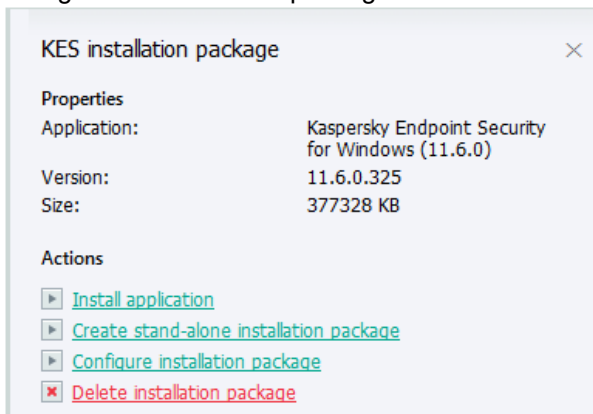
← New Package Wizard ×



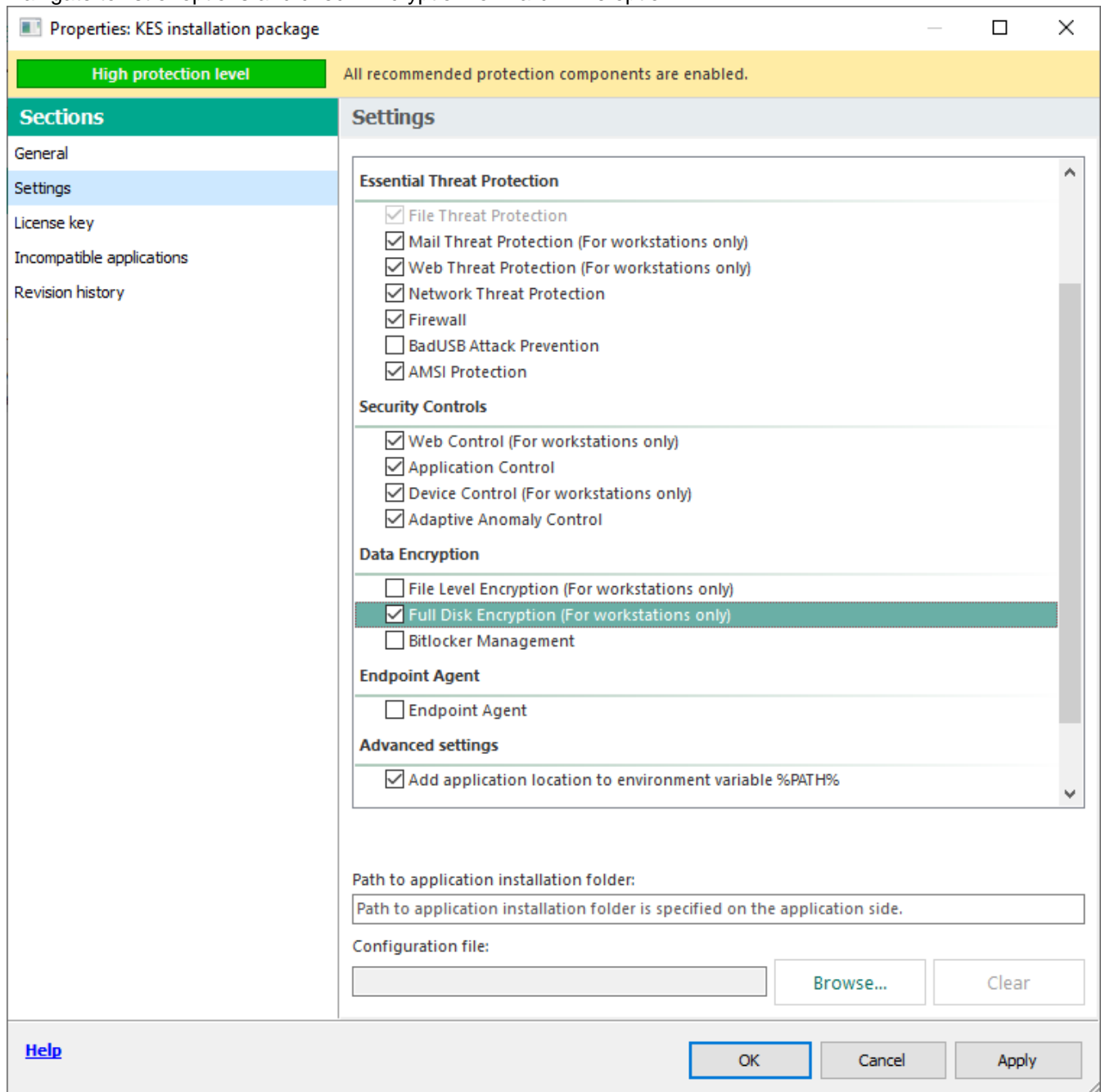
Installation package "New installation package" for "Kaspersky Endpoint Security for Windows (11.6.0) 11.6.0.325" has been successfully created.

Finish

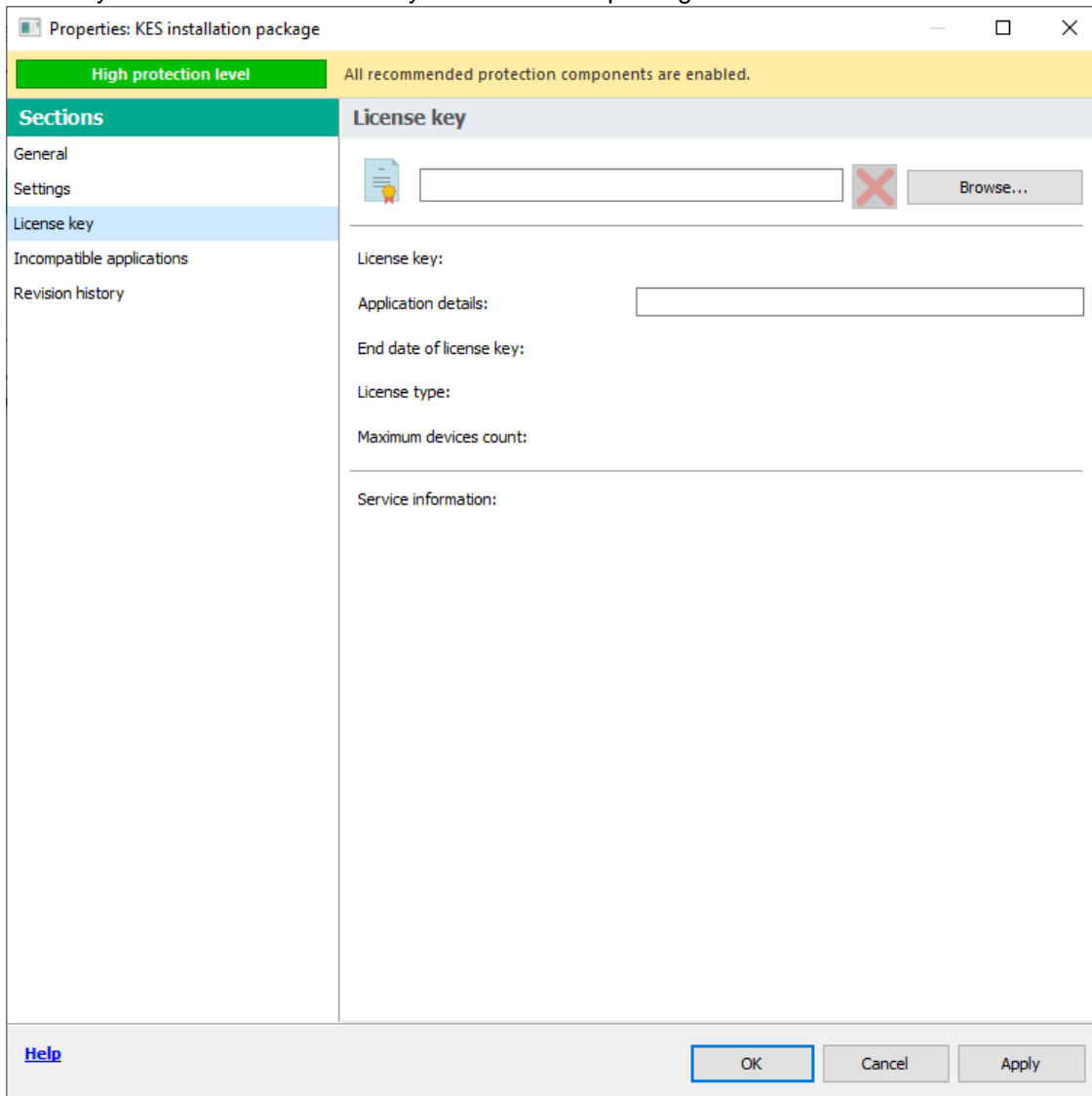
Navigate to “Installation packages” windows. Select the package and click Configure Installation package.



Navigate to list of options and check Encryption for Hard Drive option.



You may also include Activation key into installation 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.

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 TLS protocol.	Numerical value
USESSL	Whether to use TLS connection	<ul style="list-style-type: none"> • 1 – Use • Other value or no value – Do not use
OPENUDPPOINT	Whether to open a UDP port	<ul style="list-style-type: none"> • 1 – Open • Other value or no value – Do not open
UDPPOINT	UDP port number	Numerical value
USEPROXY	Whether to use a proxy server	<ul style="list-style-type: none"> • 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:	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 1 – Enable • Other value or no value – Do not enable
LAUNCHPROGRAM	Whether to run the Network Agent service after installation completion	<ul style="list-style-type: none"> • 1 – Run • Other value or no value – Do not ru

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

kaspersky

www.kaspersky.com/
www.securelist.com

© 2021 AO Kaspersky Lab.

All rights reserved. Registered trademarks and service marks are the property of their respective owners