Kaspersky Endpoint Security for Windows

(version 11.6.0.394 AES256)

Preparative Procedures

Document version: 2.03

26.11.2021

Table of Contents

1 A	bout this	s document	4
1.1	Term	inology	4
1.2	Refer	ences	4
2 In	ntroducti	on	5
2.1	ST R	eference	5
2.2	Produ	uct Reference	5
2.3	Requ	irements and prerequisites	5
2.	.3.1	Hardware	5
2.	.3.2	Software	5
2.	.3.3	KSC management software	5
3 S	ecurity (Objectives	6
3.1	KSC	management	6
3.2	TOE	secure operation	6
3.3	Trust	ed administration	6
3.4	Corre	ect behaviour of authorised users	6
4 P	reparati	ve procedures	7
4.1	OS s	etup	7
4.	.1.1	Secure Boot has to be enabled on supported systems	7
4.	.1.2	Safe mode boot for OS is disabled	7
4.2	Chec	k installation package	7
4.3	Kasp	ersky Security Center (KSC)	7
4.	.3.1	KSC installation	7
4.	.3.2	KSC settings	7
4.	.3.3	Set up KSC connection	8
4.	.3.4	Install management plug-in	8
4.4	Produ	uct Installation	8
4.	.4.1	Manual installation	8
4.	.4.2	Remote installation	9
4.	.4.3	Install activation keys	9
4.	.4.4	Upgrade from previous version	9
4.5	Set u	p policies for Kaspersky Endpoint Security for Windows	9
4.	.5.1	Setup settings password protection	9
4.	.5.2	Create encryption policy	9
4.	.5.3	Disable local Tasks	11
4.6	Confi	gure organization-specific settings	11
4.	.6.1	Create relevant access policies	11
4.	.6.2	Create AV settings	12
4.	.6.3	Group tasks	12
4.7	Apply	policies for Kaspersky Endpoint Security for Windows	12

4.7.1	Apply created policy	12
4.7.2	Verify that encryption tasks are finished on endpoint machines	13
4.8 Crea	te 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. Inst	allation walkthrough	18
Annex 2. Rer	note Installation	23
Annex 3. Inst	alling 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

ī

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
 - o 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: <u>https://www.kaspersky.com/small-to-medium-business-security/downloads/security-center</u>



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:

 Administration Server
 Administration Server properties View information about Administration Server key Configure functionality displayed in user interface
Configure interface ? ×
 Display Systems Management Display data encryption and protection Display endpoint control settings Display Mobile Device Management Display slave Administration Servers Display security settings sections
OK Cancel



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 klcfginst.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.

K Support			-	×
	Kaspersky Endpoin	t Security		0
	License key:	4228F053-2C84-4FA1-9DE4-85E68E19A33A		
kaspersky	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		
	Knowledge Rase			



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.

K Enter the administrator password	0 ×		
At leas At leas 1. Lati 2. Lati 3. Nur	commended to use a strong pass 3 characters; pone symbol from each of these categories: uppercase letters owercase letters ers I characters: (~!@#%^*{}[]<>?;':",/\=+)	is ^{its} sword. A strong passw	ord should contain:

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: !::,."Ne% 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



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 com 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 devices. If a device already has any data stored on it, it is recommended to encrypt the en- Use Legacy USB Support (not recommended) 	o use this function for new, unused
Exclusions	
Description of the second seco	
Password settings Configure passwords for Authentication Agent Block password after	failed input attempt(s) (1-20)
Configure passwords for Authentication Agent	failed input attempt(s) (1-20)
Configure passwords for Authentication Agent Configure password after 5	failed input attempt(s) (1-20)
Configure passwords for Authentication Agent Configure password after S Use Single Sign-On (SSO) technology	failed input attempt(s) (1-20)
Configure passwords for Authentication Agent Configure password after S Use Single Sign-On (SSO) technology Minimum password length (1-50 characters)	failed input attempt(s) (1-20)
Configure passwords for Authentication Agent Block password after 5 Use Single Sign-On (SSO) technology Minimum password length (1-50 characters) 8	failed input attempt(s) (1-20)

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 displa	yed			
 Allow management of group t 	asks			

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

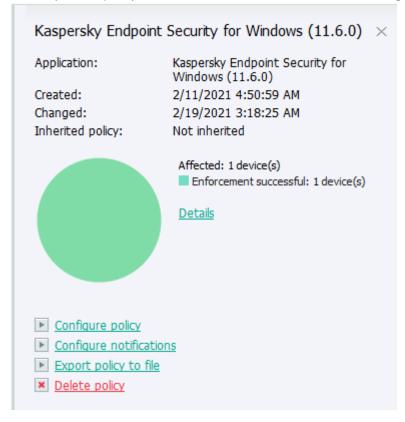
Create group tasks for different AV scans that users will be able to execute manually.

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.



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.

GENERAL APPLICATIONS ACTIVE PO	LICIES AND POLICY PROFILES TASKS	EVENTS INCIDENTS TAGS ADVANCED
General Network System Protection Device status defined by application	Visible Device status Status description Protection status Last full scan Virus detected	Yes Warning Restart is required Running 09/17/2021 2:21:10 pm
	Objects that have failed disinfection Encryption Disk encryption status <u>View data encryption errors</u>	0 Applying the policy restart is required

Authentication agent

kaspersky

Full disk encryption compatibility test.

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

Click Continue or press any key to start Windows.

CONTINUE

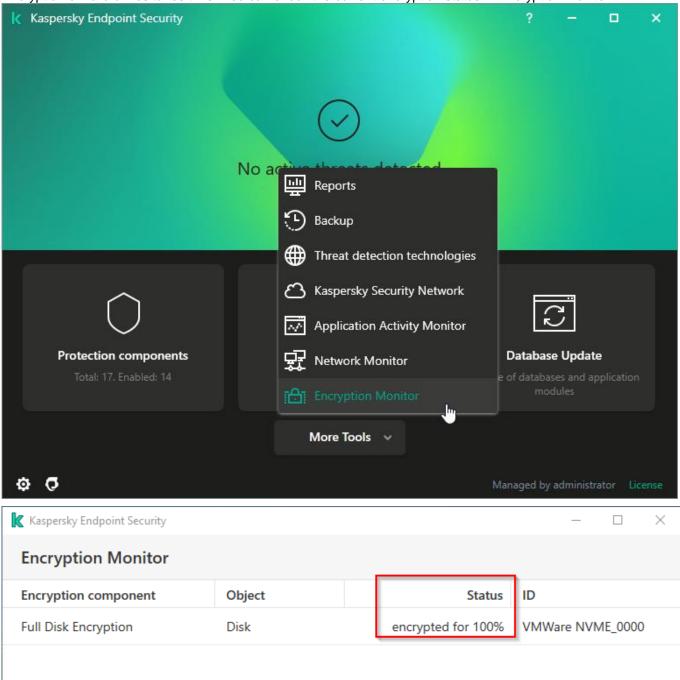
DESKTOP-Q9N1073

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.



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

GENERAL APPLICATIONS ACTI	IVE POLICIES	SAND POLICY PROFILES	TASKS	EVENTS	INCIDENTS	TAGS	ADVANCED
General Network System		Visible Device status Status description		Yes OK			
Protection		Protection status Last full scan		Running 09/17/20)21 2:21:10 pm		
Device status defined by application	1	Virus detected Objects that have failed d	isinfection	0			
		Encryption Disk encryption status View data encryption error	<u>ors</u>	Meets th	e 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 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.

4	New Task Wizard		\$		×
	Update sources				
	Add C Edit C Delete	Move up	Move down		
				<u>N</u> ext Cance	el

Annex 1. Installation walkthrough

1. Unzip obtained package to created temporary directory.

Name	Date modified	Туре	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. 5.

User Account Control			\times	
Do you want to allow this app to make				
changes to your device?				
, , , , , , , , , , , , , , , , , , ,				
Kaspersky Endpoint	Security 11	for Windo	ows	
Verified publisher: Kaspersky Lab JSC File origin: Hard drive on this computer				
Show more details				
Yes		No		
Setup will start.				
Read and accept End User	License Ag	greement.		
🖟 Kaspersky Endpoint Security for Wind	lows	—		×
End User License Agreement				
Please read the following License Agreeme	nt carefully.			
Kaspersky Endpoint Security, AES En Agent END USER LICENSE AGREEM PRIVACY POLICY				
Agent END USER LICENSE AGREEM	ENTS; AND Pro	ducts and Serv	vices	^
Agent END USER LICENSE AGREEM PRIVACY POLICY Kaspersky Endpoint Security and Kas LICENSE AGREEMENTS IMPORTANT LEGAL NOTICE TO AI FOLLOWING LEGAL AGREEMENT F	ENTS; AND Pro spersky Endpoin LL USERS: CARE BEFORE YOU ST	ducts and Serv t Agent END U EFULLY READ ART USING T	THE THE	~
Agent END USER LICENSE AGREEM PRIVACY POLICY Kaspersky Endpoint Security and Kas LICENSE AGREEMENTS IMPORTANT LEGAL NOTICE TO AI	ENTS; AND Pro spersky Endpoin LL USERS: CARE BEFORE YOU ST	ducts and Serv t Agent END U EFULLY READ ART USING T	THE THE	~
Agent END USER LICENSE AGREEM PRIVACY POLICY Kaspersky Endpoint Security and Kas LICENSE AGREEMENTS IMPORTANT LEGAL NOTICE TO AI FOLLOWING LEGAL AGREEMENT E	ENTS; AND Pro spersky Endpoin LL USERS: CARH BEFORE YOU ST tand, and accept t be handled and tr	ducts and Serv t Agent END U EFULLY READ ART USING T he terms and cor ansmitted (includ	THE HE nditions of th	~
Agent END USER LICENSE AGREEM PRIVACY POLICY Kaspersky Endpoint Security and Kas LICENSE AGREEMENTS IMPORTANT LEGAL NOTICE TO AI FOLLOWING LEGAL AGREEMENT F I confirm that I have fully read, underst End User License Agreements I am aware and agree that my data will Countries) as described in the Privacy P	ENTS; AND Pro spersky Endpoin LL USERS: CARH BEFORE YOU ST tand, and accept t be handled and tr	ducts and Serv t Agent END U EFULLY READ ART USING T he terms and cor ansmitted (includ	THE HE nditions of th	~

6. In the next screen scroll down and choose "Full Disk Encryption" option to be installed.

Kaspersky Endpoint Security for Windows - ×			
Custom installation Select the application features that you want to install.			
Kaspersky Endpoint Security for Windows Application core, including scan tasks Advanced Threat Protection Essential Threat Protection Security Controls Data Encryption Y File Level Encryption Full Disk Encryption			~
Allows encryption of hard drives and removable drives. Feature installation requires 121 MB on the local hard drive.		Volume	
© 2021 AO Kaspersky Lab Help Reset < Back Next :	>	Can	icel

7. Leave destination folder as offered by the setup.

Haspersky Endpoint Security for Windows	-		×
Select destination folder Please select the folder to which the application will be installed.			
To install the application to the specified folder, dick Next. To ins select it by using the Browse button.	tall to a differ	ent folder,	
Destination folder:	1.0.1		
ogram Files (x86) (Kaspersky Lab (Kaspersky Endpoint Security fo	or Windows\	Browse.	
© 2021 AO Kaspersky Lab			
Volume < Back	Next >	Cano	el

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

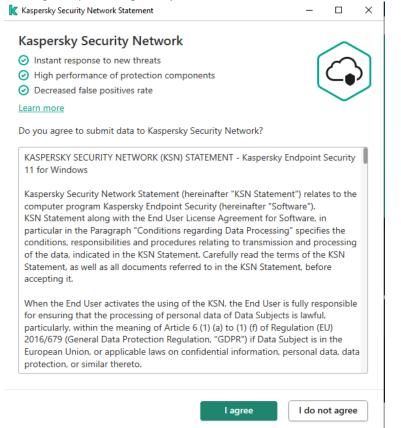
🖟 Kaspersky Endpoint Security for Windows	-		×
Ready to install Please confirm that you are ready to install the application.			
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the Wizard.			
Attention! Network or Internet connections may be interrupted, and operating system notifications may be displayed during application setup.			
Protect the application installation process			
Ensure compatibility with Citrix Provisioning Services (this is only necessary when working with Citrix PVS)			
Recommended actions after the application installation is complete:			
Add the path to the file avp.com to the system variable %PATH%			
© 2021 AO Kaspersky Lab			
< Back Install		Can	cel

9. Installation process will start...

🕼 Kaspersky Endpoint Security for Windows	—		\times
Installation in progress The application is being installed. Please wait			
Copying new files			
© 2021 AO Kaspersky Lab			
		Cance	el
10and finish. KES is installed			
🔀 Kaspersky Endpoint Security for Windows			

kaspersky	Finished the application Setup Wizard.
	The Setup Wizard has completed successfully.
	Finish

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.

<u>k</u> Kaspersky E	ndpoint Security	•	?		0	×
← Licens	ing					
	Key: License: Application name: Functionality:	 Trial license for 10 computers Kaspersky Endpoint Security for workstations and file Protection Security Controls Data Encryption 	e server	s		
	Attention! Trial licer the full version of the Delete key Purchase license Visit online store to purch		ou purcl	hase a li	icense fo)r
\$ (7					Li	cense

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

Kaspersky Endpoint Security		?	_	٥	×
← Activation	~				
Activate with an activation code					
Activation code format: XXXXX-XXXXX-XXXXX-XXXXX. If you do not have an activation code, you can purchase it <u>on the website</u> .					
You can copy the entire activation code and paste it into the first entry field without ty The activation code is not case-sensitive.	ping characters i	manually.			
Activate					
Activate with a key file					
Key file is required.					
Select key file					
\$ 7				Li	cense

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.

 \times

÷	New Package	Wizard
	Select install	ation package type
		Create an installation package for a Kaspersky application.
		Create an installation package for the specified executable file.
		Select an application from the Kaspersky database to create an installation package.

Cancel

Select Create an installation package for a Kaspersky application.

		X
←	New Package Wizard	
	Defining the installation package name	
	Name:	
	KES installation package	
		Next Cancel

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.

w Package Wizard			
cting the distribution package for installation			
Kaspersky Endpoint Security for Windows (11.6.0)	Browse		
Application version: 11.6.0.325			
anguage: en			
Copy updates from repository to installation package			
		_	
	Next Cancel		
	Next Cancel		
eck "Copy updates from repository"		ext.	
eck "Copy updates from repository"		ext.	
eck "Copy updates from repository" New Package Wizard			
	checkbox. Click Ne		
New Package Wizard	checkbox. Click Ne		
New Package Wizard nd User License Agreement and Privacy Policy aspersky Endpoint Security, AES Encryption Module and Kaspersi	checkbox. Click Ne		
New Package Wizard Ind User License Agreement and Privacy Policy aspersky Endpoint Security, AES Encryption Module and Kaspers ICENSE AGREEMENTS; AND Products and Services PRIVACY POL	checkbox. Click Ne	×	
New Package Wizard Ind User License Agreement and Privacy Policy aspersky Endpoint Security, AES Encryption Module and Kaspersi ICENSE AGREEMENTS; AND Products and Services PRIVACY POL aspersky Endpoint Security and Kaspersky Endpoint Agent END L MPORTANT LEGAL NOTICE TO ALL USERS; CAREFULLY READ TH	checkbox. Click Ne	×	
New Package Wizard aspersky Endpoint Security, AES Encryption Module and Kaspers ICENSE AGREEMENTS; AND Products and Services PRIVACY POL aspersky Endpoint Security and Kaspersky Endpoint Agent END L WPORTANT LEGAL NOTICE TO ALL USERS; CAREFULLY READ THE EFORE YOU START USING THE SOFTWARE.	checkbox. Click Ne	×	
New Package Wizard aspersky Endpoint Security, AES Encryption Module and Kaspersi ICENSE AGREEMENTS; AND Products and Services PRIVACY POLI aspersky Endpoint Security and Kaspersky Endpoint Agent END L WPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THI EFORE YOU START USING THE SOFTWARE. LICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE Y GREEMENT, OR BY ENTERING CORRESPONDING SYMBOL(-S), Y	Checkbox. Click Ne	SE	
New Package Wizard Ind User License Agreement and Privacy Policy aspersky Endpoint Security, AES Encryption Module and Kaspersi ICENSE AGREEMENTS; AND Products and Services PRIVACY POL aspersky Endpoint Security and Kaspersky Endpoint Agent END L MPORTANT LEGAL NOTICE TO ALL USERS; CAREFULLY READ THE EFORE YOU START USING THE SOFTWARE. LICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE 10	Checkbox. Click Ne	SE	
New Package Wizard aspersky Endpoint Security, AES Encryption Module and Kaspersi ICENSE AGREEMENTS; AND Products and Services PRIVACY POL aspersky Endpoint Security and Kaspersky Endpoint Agent END L WPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE EFORE YOU START USING THE SOFTWARE. LICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE IN GREEMENT, OR BY ENTERING CORRESPONDING SYMBOL (-5), YU YAY THAT YOU AS THE ORGANIZATION FOR WHICH THE SOFTW CQUIRED HAVE AUTHORIZED THE NATURAL PERSON ACCEPTIN INTER INTO THIS LICENSE AGREEMENT FOR AND ON BEHALF OF IONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THE CITION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSI	Checkbox. Click Ne checkbox. Click Ne cy Endpoint Agent END USER (cy user LICENSE AGREEMENTS E FOLLOWING LEGAL AGREEMENT DU CONFIRM IN A LEGALLY BINDIN ARE IS DOWNLOADED OR G THIS LICENSE AGREEMENT TO YOU, FURTHERMORE, YOU IS LICENSE AGREEMENT. SUCH SNITING TO BE DOUND BY AND ARE IS DOWNLOADED OR SILICENSE AGREEMENT. SUCH SILICENSE AGREEMENT. SUCH SNITING TO BE DOUND BY AND ARE	SE	
New Package Wizard Ind User License Agreement and Privacy Policy aspersky Endpoint Security, AES Encryption Module and Kaspersi ICENSE AGREEMENTS; AND Products and Services PRIVACY POL aspersky Endpoint Security and Kaspersky Endpoint Agent END L MPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE EFORE YOU START USING THE SOFTWARE. LICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE I GREEMENT, OR BY ENTERING CORRESPONDING SYMBOL(-S), YO UAY THAT YOU AS THE ORGANIZATION FOR WHICH THE SOFTWARE. LICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE I GREEMENT, OR BY ENTERING CORRESPONDING SYMBOL(-S), YO UAY THAT YOU AS THE ORGANIZATION FOR WHICH THE SOFTWARE. LICKING THE BUTTON BY THE TERNS AND CONDITIONS OF THI COUJIRED HAVE AUTHORIZED THE NATURAL PERSON ACCEPTING NOTENT TO BE BOUND BY THE TERNS AND CONDITIONS OF THIS CONSENT TO BE BOUND BY THE TERNS AND CONDITIONS OF THIS COMING A PARTY TO THIS LICENSE AGREEMENT FOR AND VID ARE CONSI ECOMING A PARTY TO THIS LICENSE AGREEMENT AND AGREET NFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT FOR AND AGREEMENT FOR AND AGREEMENT FOR AND AGREEMENT SING COMING A PARTY TO THIS LICENSE AGREEMENT FOR AND CONDITIONS OF THE NFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT FOR AND AGREEMENT FOR AND AGREEMENT FOR AND AGREEMENT FOR AND AGREEMENT FOR AND AGREEMENT FOR AND CONDITIONS OF THE COMING A PARTY TO THIS LICENSE AGREEMENT FOR AND AGREEMENT FOR NFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT FOR AND AGREEMENT FOR AND AGREEMENT FOR AND CONDING SOFT TO COMING A PARTY TO THIS LICENSE AGREEMENT FOR AND AGREEMENT FOR NFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT FOR NFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT FOR COMING A PARTY FOR THE FORMANCE AND FOR FORMENT FOR AGREEMENT FOR AGREEMENT FOR AGREEMENT FOR AGREEMENT FOR A FORMANCE AND AGREEMENT FOR AGREEMENT FOR A FORMANCE AND FORMANCE A FORMANCE AND FORMANCE A FORMANCE AND FORMANCE AND FORMANCE AND AG	checkbox. Click Ne cy Endpoint Agent END USER (/ / / / / / / / / / / / / /	SE	
New Package Wizard aspersky Endpoint Security, AES Encryption Module and Kaspersl ICENSE AGREEMENTS; AND Products and Services PRIVACY POLI aspersky Endpoint Security and Kaspersky Endpoint Agent END L WPORTANT LEGAL NOTICE TO ALL USERS; CAREFULLY READ THE EFORE YOU START USING THE SOFTWARE. LICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE 1 IGREEMENT, OR BY ENTERING CORRESPONDING SYMBOL, (S), YV VAY THAT YOU AS THE ORGANIZATION FOR WHICH THE SOFTW CQUIRED HAVE AUTHORIZED THE NATURAL PERSON ACCEPTIN INTER INTO THIS LICENSE AGREEMENT FOR AND ON BEHALF OF IONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THI ICTION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSI ECOMING A PARTY TO THIS LICENSE AGREEMENT AND AGREET	Checkbox. Click Ne checkbox. Click Ne cy Endpoint Agent END USER (cy iser LICENSE AGREEMENTS E FOLLOWING LEGAL AGREEMENT VINDOW CONTAINING THE LICEN DU CONFIRM IN A LEGALLY BINDIN ARE IS DOWNLOADED OR G THIS LICENSE AGREEMENT TO YOU. FURTHERMORE, YOU S LICENSE AGREEMENT TO YOU. FURTHERMORE, YOU S LICENSE AGREEMENT TO YOU. FURTHERMORE, YOU S LICENSE AGREEMENT IS NED BY YOU. IF YOU DO NOT LAGREEMENT, CANCEL THE	SE	
New Package Wizard aspersky Endpoint Security, AES Encryption Module and Kaspersi ICENSE AGREEMENTS; AND Products and Services PRIVACY POL aspersky Endpoint Security and Kaspersky Endpoint Agent END L WPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE EFORE YOU START USING THE SOFTWARE. LICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE N GREEMENT, OR BY ENTERING CORRESPONDING SYMBOL (-S), YK VAY THAT YOU BY ENTERING CORRESPONDING SYMBOL (-S), YK VAY THAT YOU BY ENTERING CORRESPONDING SYMBOL (-S), YK UNITER INTO THIS LICENSE AGREEMENT FOR AND ON BEHALF OF CONSENT TO BE BOUIND BY THE TERMS AND CONDITIONS OF THE CITION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSI ECOMING A PARTY TO THIS LICENSE AGREEMENT AND AGREET T NFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT FIG GREETO ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE	Checkbox. Click Ne cy Endpoint Agent END USER (y cy Endpoint Agent END USER (cy ISER LICENSE AGREEMENTS FOLLOWING LEGAL AGREEMENT STOLOWING LEGAL AGREEMENT STOLOWING LEGAL AGREEMENT STOLOWING AGREEMENT, SUCH STOL CONFIRM IN A LEGALLY BINDIN ARE IS DOWNLOADED OR G THIS LICENSE AGREEMENT TO YOU. FURTHERMORE, YOU S LICENSE AGREEMENT, SUCH MAT THIS LICENSE AGREEMENT IS NED BY YOU. IF YOU DO NOT E AGREEMENT, CANCEL THE FTWARE. COFTWARE, TERMS OF THE	SE IG	
New Package Wizard aspersky Endpoint Security, AES Encryption Module and Kaspersi ICENSE AGREEMENTS; AND Products and Services PRIVACY POLI aspersky Endpoint Security and Kaspersky Endpoint Agent END L WPORTANT LEGAL NOTICE TO ALL USERS; CAREFULLY READ THI EFORE YOU START USING THE SOFTWARE. LICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE 1 IGREEMENT, OR BY ENTERING CORRESPONDING SYMBOL (-S), YO IGREEMENT, OR BY ENTERING CORRESPONDING SYMBOL (-S), YO INTAT YOU AS THE ORGANIZATION FOR WHICH THE SOFTW COURSED HAVE AUTHORIZED THE NATURAL PERSON ACCEPTIN ITER INTO THIS LICENSE AGREEMENT FOR AND ON BEHALF OF CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THI CITON IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSI ECOMING A PARITY TO THIS LICENSE AGREEMENT FOR AND ON BEHALF OF NFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIG GREETO ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE NSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFT NSTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFT ICCENSE CONTRACT OR SIMILAR DOCUMENT ACCOMPANIES SOFT ICCENSE CONTRACT OR SIMILAR DOCUMENT ACCOMPANIES	Checkbox. Click Ne checkbox. Click Ne cy Endpoint Agent END USER (cy user LICENSE AGREEMENTS E FOLLOWING LEGAL AGREEMENT DU CONFIRM IN A LEGALLY BINDIN ARE IS DOWNLOADED OR G THIS LICENSE AGREEMENT TO YOU, FURTHERMORE, YOU IS LICENSE AGREEMENT. SUCH SILICENSE AGREEMENT. SUCH SILICENSE AGREEMENT. SUCH SILICENSE AGREEMENT. SUCH SILICENSE AGREEMENT. SUCH SILICENSE AGREEMENT. SUCH SILICENSE AGREEMENT. CANCEL THE ETWARE. IOFTWARE, TERMS OF THE E CURRENT LICENSE AGREEMENT.	SE IG	
New Package Wizard aspersky Endpoint Security, AES Encryption Module and Kaspersi ICENSE AGREEMENTS; AND Products and Services PRIVACY POL aspersky Endpoint Security and Kaspersky Endpoint Agent END L MPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE EFORE YOU START USING THE SOFTWARE. LICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE 1 GREEMENT, OR BY ENTERING CORRESPONDING SYMBOL(-S), YU 400 HAVE AUTHORIZED THE NATURAL PERSON ACCEPTIN CQUIRED HAVE AUTHORIZED THE NATURAL PERSON ACCEPTIN NTER INTO THIS LICENSE AGREEMENT FOR AND ON BEHALF OF CONSENT TO BE BOUND BY THE TERNS AND CONDITIONS OF THI CITION IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSI GREE TO ALL OF THE TERMS AND CONDITIONS OF THIS LICENS INFORCEABLE LIKE ANY WRITTEN INEGOTIATED AGREEMENT SIG GREE TO ALL OF THE TERMS AND CONDITIONS OF THIS LICENS USTALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SO F LICENSE CONTRACT OR SIMILAR DOCUMENT ACCOMPANIES SO OFTWARE USE DEFINED IN SUCH DOCUMENT PREVAIL OVER TH	Checkbox. Click Ne	SE IG	
New Package Wizard Ind User License Agreement and Privacy Policy aspersky Endpoint Security, AES Encryption Module and Kaspersi ICENSE AGREEMENTS; AND Products and Services PRIVACY POL aspersky Endpoint Security and Kaspersky Endpoint Agent END L WPORTANT LEGAL NOTICE TO ALL USERS: CAREFULLY READ THE EFORE YOU START USING THE SOFTWARE. LICKING THE BUTTON INDICATING YOUR ACCEPTANCE IN THE 1 GREEMENT, OR BY ENTERING CORRESPONDING SYMBOL (-S), YO AY THAT YOU AS THE ORGANIZATION FOR WHICH THE SOFTW CQUIRED HAVE AUTHORIZED THE NATURAL PERSON ACCEPTIN INTER INTO THIS LICENSE AGREEMENT FOR AND ON BEHALF OF CONSENT TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS CITON IS A SYMBOL OF YOUR SIGNATURE AND YOU ARE CONSE ECOMING A PARTY TO THIS LICENSE AGREEMENT FOR AND ON BEHALF OF NFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIG GREE TO ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE NFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIG GREE TO ALL OF THE TRMS AND CONDITIONS OF THIS LICENSE NFALLATION OF THE SOFTWARE AND DO NOT INSTALL THE SOFTWARE AND CONDITIONS OF THIS LICENSE OFTWARE USE DEFINED IN SUCH DOCUMENT ACCOMPANIES SOFTWARE USE DEFINED IN SUCH DOCUMENT REVAIL OVER TH FTER CLICKING THE ACCEPT BUTTON IN THE WINDOW CONTAL	checkbox. Click Net checkbox. Click Net (ry Endpoint Agent END USER (CY iser LICENSE AGREEMENTS FOLLOWING LEGAL AGREEMENT SE FOLLOWING LEGAL AGREEMENT OU CONFIRM IN A LEGALLY BINDIN ARE IS DOWNLOADED OR G THIS LICENSE AGREEMENT TO UCONFIRM THA ALEGALLY BINDIN ARE IS DOWNLOADED OR G THIS LICENSE AGREEMENT TO IS LICENSE AGREEMENT SUCH NITING TO BE BOUND BY AND ARE NED BY YOU, JF YOU DO NOT E AGREEMENT, CANCEL THE FTWARE. IOFTWARE, TERMS OF THE E CURRENT LICENSE AGREEMENT O and conditions of the following:	SE IG	

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	
Wai	t until the package is created.		
			×
~	New Package Wizard		
	Installation package "New installation package" for "Kaspersky Windows (11.6.0) 11.6.0.325" has been successfully created	y Endpoint Security for	
	•		

Finish



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

KES installation package		×
Properties		
Application:	Kaspersky Endpoint Security for Windows (11.6.0)	
Version:	11.6.0.325	
Size:	377328 KB	
Actions		
Install application		

Create stand-alone installation package

<u>Configure installation package</u>

Delete installation package

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

Properties: KES installation package		—		×
High protection level	All recommended protection components are enabled.			
Sections	Settings			
General				
Settings	Essential Threat Protection			^
License key	File Threat Protection			
Incompatible applications	 Mail Threat Protection (For workstations only) Web Threat Protection (For workstations only) 			
Revision history	Network Threat Protection			
	 ☐ Firewall			
	BadUSB Attack Prevention			
	AMSI Protection			
	Security Controls			
	Web Control (For workstations only)			
	Application Control			
	Device Control (For workstations only) Adaptive Anomaly Control			
	Data Encryption			
	 File Level Encryption (For workstations only) ✓ Full Disk Encryption (For workstations only) 			
	Bitlocker Management			
	Endpoint Agent			
	Endpoint Agent			
	Advanced settings			
	Add application location to environment variable %PATH%			~
	Path to application installation folder:			
	Path to application installation folder is specified on the application side.			
	Configuration file:			
	Browse		Clear	
<u>Help</u>	OK Cancel		Apply	



You may also include Activation key into installation package.

Properties: KES installation package	— 🗆 X
High protection level	All recommended protection components are enabled.
Sections	License key
General	Browse
Settings	Browse
License key	
Incompatible applications	License key:
Revision history	Application details:
	End date of license key:
	License type:
	Maximum devices count:
	Service information:
Help	
	OK Cancel Apply

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	 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 objectives USESSL parameter should be set to 1.



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