Kaspersky Internet Security 2014: Reviewer's Guide

KASPERSKY lab

Index

This guide explains how to use Kaspersky Internet Security 2014 (KIS 2014) - an integrated product providing system protection for Microsoft Windows 8. XP, Windows 7, Vista and Windows XP against malware, Trojans, hacker attacks, spam, spyware, phishing, confidential data leaks and undesirable content.

1 Introduction

Kaspersky Internet Security 2014 delivers premium PC protection from all Internet threats, including the most sophisticated of them, ensuring you're always safe as you use the web to bank, shop, surf, social network, and more. Unique technologies, such as Safe Money and Secure Keyboard, protect your financial transactions via online banks, payment systems such as PayPal, and e-stores. Automatic Exploit Prevention and ZETA Shield technologies effectively prevent attacks via vulnerabilities in operating systems and popular applications, as well as so-called **targeted attacks**. Unique Trusted Applications Mode allows users to work in an absolutely trusted environment where only legitimate applications can be launched. Plus, Kaspersky Internet Security 2014 is optimized for maximum performance, so you'll never be slowed down as you use the Internet to its full potential.

You can find additional information about targeted attacks here

2 Key Benefits

2.1 Real-time protection against all Internet threats

The Internet gives us tremendous freedom and convenience – to shop, bank, keep up with friends, download music, share pictures, etc. at any time of day or night and from just about anywhere. But, it can also leave us vulnerable to viruses and other Internet threats that are continually popping up – at a rate of around 200,000 new pieces of malware every day.

Our innovative **hybrid approach** to protection combines the real-time efficiency of the cloud with powerful security technologies on your PC to deliver a faster, more effective response to today's complex, ever-evolving threats.

KIS 2014 includes a set of updated technologies to provide full protection for your computer during all kinds of online activity. Examples include: **Safe Money** technology to protect personal data during financial transactions; **Secure Keyboard** mode to protect data entered via a physical keyboard; **Anti-phishing protection** to keep your personal data safe from hackers; and **URL Advisor**, which advises you of the danger level of web links.

Kaspersky Lab research on the evolution of malware attacks is available here

2.2 Secure online banking and shopping

Kaspersky Internet Security 2014 provides additional layers of protection during financial transactions, such as online banking, using payment systems (e.g. PayPal), and making purchases on e-commerce sites. Our unique **Safe Money** technology will ensure the website is secure and that you're not being tricked by a fake or **phishing website**. And, it will offer to open the website in a special protected mode, keeping your credit card number and other personal data safe from cyber-thieves.

Our new **Secure Keyboard** activates automatically when you open a bank or payment website or enter a password within any web page, protecting any information you enter via a physical keyboard from keyloggers. And, for the complete protection of personal information when banking online, we've implemented fast access to the **Virtual Keyboard** from web browsers. Virtual Keyboard allows you to use mouse clicks to enter your banking information, so they can't be tracked or stolen by keyloggers, hackers or identity thieves.

You can find the latest estimates of the volume of phishing attacks here

2.3 Proactive protection against unknown threats

One of the easier ways for cybercriminals to find holes in users' protection is through **application and system vulnerabilities** that haven't been updated with the latest fixes. For example, popular programs such as Adobe Reader, Internet Explorer, and Firefox, Java applications, etc., can offer an easy gateway for malicious programs. Kaspersky Internet Security 2014 includes Automatic Exploit Prevention that not only scans for vulnerabilities – it analyzes and controls the actions that programs and applications perform with vulnerabilities so they can't cause any harm. Also nowadays new malware is appearing at an incredibly fast rate – currently around 200,000 new samples every day – meaning traditional signature analysis alone is no longer enough to combat it effectively. This is why proactive protection is a primary means of defense, analyzing the behavior of applications and blocking them if they appear suspicious.

KIS 2014 includes **System Watcher** technology that monitors and logs the activity of all applications in the system, analyzes their behavior, and blocks any undesirable actions. **System Watcher** also allows you to roll back the actions of malware.

The additional information about vulnerabilities in popular applications is available in Kaspersky Lab report

2.4 Ensures the applications on your PC are safe

For an extra level of protection, Kaspersky Internet Security 2014 offers a new **Trusted Applications Mode**. It uses the Kaspersky Whitelisting service, which designates "trusted" applications that Kaspersky Lab guarantees are safe. All other applications are restricted when this mode is turned on.

2.5 On the way to 'cloud' protection

The software security landscape is changing at an ever-increasing rate and the fact that tens of thousands of new cybercrime threats are appearing every day means the rules for effective software security have changed. To react promptly to new threats, KIS 2014, as in the previous version, includes **Kaspersky Security Network**, a system of online databases on Kaspersky Lab servers containing information about trusted, dangerous and suspicious applications. Information in the cloud is updated very quickly and then made available to all users of Kaspersky products. Each time the user runs a file on the computer, KIS refers to the cloud for up-to-date information on the application and its system rights.

KIS 2014 includes improved features to provide extensive cloud protection. **File Advisor** functionality allows you to find out the reputation of potentially dangerous files with a single mouse click. **URL Advisor** informs you about links to suspicious or dangerous websites by accessing the cloud for the latest information about online resources.

2.6 Advanced Parental Control

Parental Control is designed to protect children from **threats** on the computer and the Internet. KIS 2014 offers a wide range of functions for this purpose. It is possible to control access to the computer and Internet, control which applications can be run, limit file downloads from the Internet, control communications in social networks and game usage depending on its rating. In addition, this function can be used to view statistical reports on the actions of controlled users. In Kaspersky Internet Security 2014 the Parental Control features were significantly widened and improved. You can find a detailed description of the new features and improvements below.

The additional information about Internet threats that target children is available here

2.7 Hassle-free protection with maximum PC performance

Our driving goal is to provide you with the ultimate protection without compromising system performance or disturbing you with questions and alerts. Optimized for maximum PC performance during your active, daily use, Kaspersky Internet Security 2014 works behind-the-scenes to check the reputation of all launched applications and websites, analyze program behavior, update its databases, and more to ensure you're always safe – all without slowing down your PC.

2.8 Rescue Disk

The Rescue Disk is a boot disk that contains a set of features to detect and cure infections on your computer in situations when the operating system and antivirus software cannot be loaded as normal. The installation CD can be used for this purpose (if the box was purchased in a store), which is very convenient if a second computer is not available to download a rescue disk from the Internet.

3 Installation and Activation

KIS 2014 significantly optimizes the process of installing the product by automating much of the installation. When a user downloads and runs the product from the website, it automatically checks for the latest product version, initiates the download and installation, removes incompatible software, and performs a disinfection if anything is trying to prevent the product installation.

3.1 System requirements*

KIS 2014 is optimized to use a minimal amount of system resources. This includes:

- Operating system: Microsoft Windows 8, Windows 7, Windows Vista or Windows XP (32 or 64 bit**).
- Processor: 1 GHz CPU or higher for Windows Vista, Windows 7 or Windows 8 or 800 MHz CPU or higher for Windows XP.
- RAM: 1 GB (32-bit)/2 GB (64-bit) for Windows Vista, Windows 7 or Windows 8 or 512 MB for Windows XP.

- Disk Space: 480 MB of free space on the hard drive for installation

KIS 2014 also requires a CD-ROM drive (if the application was purchased on a CD), an Internet connection (for product activation and database updates), Internet Explorer 8 or higher, Microsoft Windows Installer 3.0 or higher and Microsoft .NET Framework 4.

* Full System requirements at: kaspersky.com.

** - - Some product features might work on 32-bit operating systems only.

You can find a complete list of system requirements at www.kaspersky.com or in the User Guide.

3.2 Installation

To begin installation of Kaspersky Internet Security 2014 on your computer, insert the installation CD into the CD/DVD drive and follow the setup wizard instructions. The Wizard consists of a series of screens (steps) that you can navigate through using the Back and Next buttons. If the **Setup Wizard** does not start automatically, run the installation file (autorun.exe) from the product CD. Before installation, the program checks the Kaspersky Lab update servers for a more recent version of Kaspersky Internet Security. If a newer version of the product is available, you will be given the option to download and install it on your computer.

Installation on an infected operating system

Sometimes a computer can be infected to such an extent that installing an antivirus solution is impossible, particularly following infection by some types of rootkits. In this case the product downloads a dedicated utility automatically and treats the system's active infections before completing the installation process.

Kaspersky Security Network

As part of the installation process, you are invited to join the **Kaspersky Security Network** (KSN). KSN automatically collects and forwards to Kaspersky Lab information about attempts to infect your computer and suspicious files detected on it (in strict anonymity and only with the user's consent). This information is sent to Kaspersky Lab for analysis and is added to our online malware database. KSN provides the very highest level of rapid threat detection.

3.3 Activation and configuration

After the **Setup Wizard** functions are complete, the **Activation Wizard** will ask you to activate the program, at which time you will need to enter the product activation code. Users who have an activation code for KIS 2013 that is still valid can use it to activate KIS 2014. An Internet connection is required to activate the application. There is no need to reboot your computer after installation. If the product was purchased via the Internet, activation is now performed automatically without the need to enter the activation code. The activation code is automatically added to KAV/KIS 2014 while downloading the product, using the link from the purchase email.

Kaspersky Lab recommends that you perform a full scan of the hard drive and all external storage devices connected to your computer immediately after installation. The duration of the first scan depends on the speed of the CPU and the number of files on the PC.

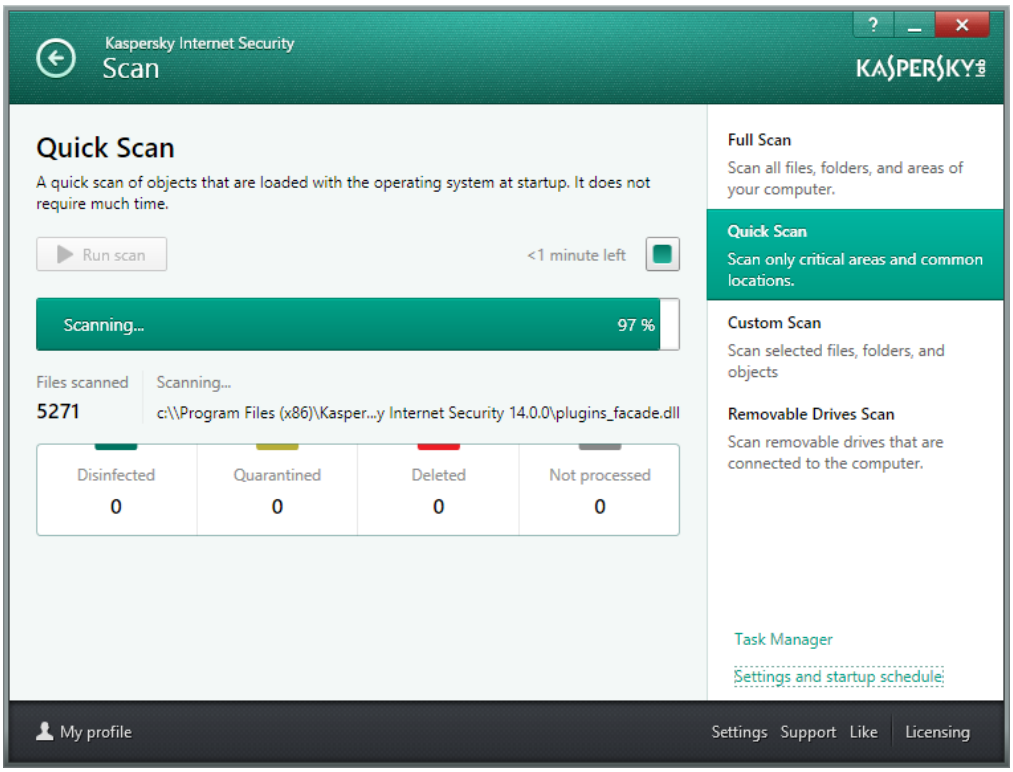
Program components

The lower part of the main window displays the main product components. By clicking on the icon with the arrow symbol, you open the full list of product components:

3.4 Scanning

Scanning the computer for viruses and vulnerabilities is one of the most important elements of security. It is vital to perform regular scans of your computer in order to rule out the spread of any malware that has not been detected by the protection components due to a customized low security setting, for example.

To scan the computer for malware, we recommend that you perform a **Full Scan** or **Quick Scan**. The **Quick Scan** covers objects that are loaded with the operating system, system memory, boot sectors on the hard drive, and other objects that you have added.



Manage Tasks

KIS 2014 allows you to view tasks executed by the application and review their status. This allows you to optimize computer resources.

3.5 Update

Updating the Kaspersky Internet Security databases and modules keeps your computer safe against the very latest threats. Every day sees the appearance of new viruses, Trojans and other malware. Information about threats and ways to neutralize them is contained in the Kaspersky Internet Security databases. Therefore, the application and its antivirus databases should be updated to safeguard your computer against new threats. KIS 2014 is updated automatically, but you can also download updates from the **Update** tab.

3.6 Safe Money – Improved!

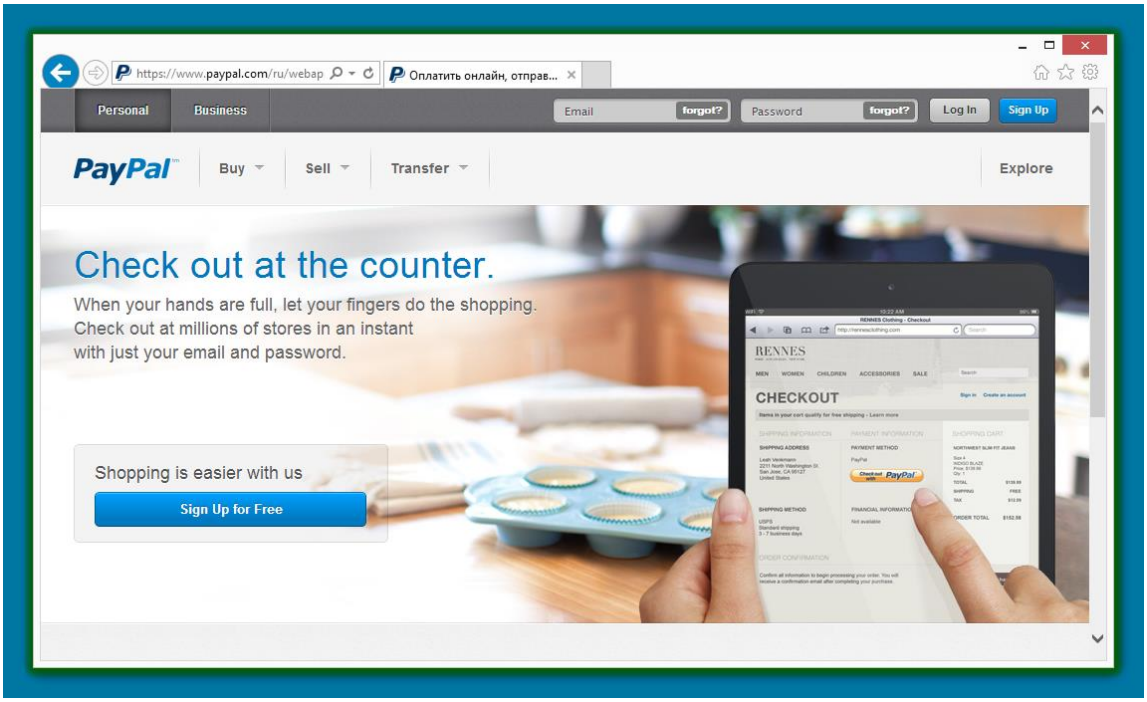
To provide protection for confidential data that you enter on banking websites and payment systems (such as banking card numbers, passwords to access online banking services), as well as to prevent theft of assets when making online payments, Kaspersky Internet Security 2014 includes unique **Safe Money** technology.

How it works:

The technology:

- Verifies that the request goes to a genuine banking or payment system site (checked against an updatable list of sites in the product).
- Verifies the security certificate, to avoid redirection to a fake website.
- Scans the operating system for vulnerabilities critical to online banking.

- Offers to open the website in **Safe Money** mode to protect your personal data against theft. In this case KIS 2014 restricts how other programs and processes can access data transferred in **Safe Money** mode, which helps to ensure protection of your personal data against theft. When **Safe Money** mode is activated, the green frame will appear around the browser window.



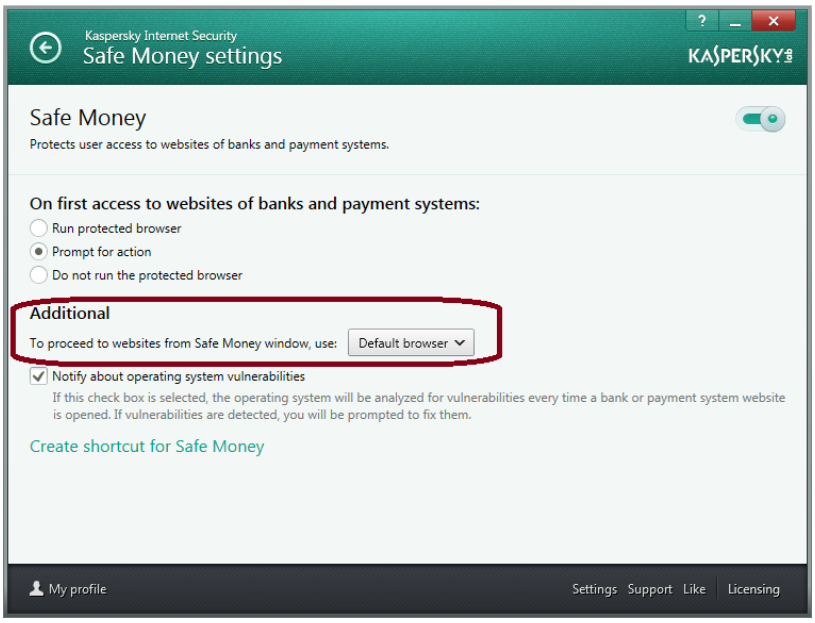
When the payment transaction via **Safe Money** is complete, the user is automatically redirected to a normal browser window to finish the process or continue shopping in the online store.

To add bank, payment or shopping sites, chose **Safe Money** in the lower part of the window and press the link **Add**.

To open the detailed settings of this feature, press the **Settings** link in the upper part of the main window and select Safe Money in the list of product components.

Safe Money Improvements in KIS 2014:

1. Ability to choose web browser.



2. Significantly increased number of shopping websites.
3. Better usability and visibility (more visible green frame around the browser window, etc).

At the same time, to protect confidential data entered via a keyboard from being intercepted, two options are available:

- **Virtual Keyboard**, which is displayed on the user's screen and controlled via the mouse.
- **Secure Keyboard**, a feature that uses a special driver to protect data input via a physical keyboard.

(Both technologies are described in detail below).

3.7 Application Control

To view the list and security rating of all applications on your PCs select **Application Control** in the lower part of the main window. To see all launched applications and running processes press link **Show all activity** in the right lower part of the **Application Control** window.

3.8 Trusted Applications Mode – New!

Controls which applications run on a user's PC based on the **Kaspersky Whitelisting service**, which designates "trusted" applications that Kaspersky Lab guarantees are safe. All other applications are restricted when this mode is turned on by the user. To turn on this mode, open **Application Control** window from the lower part of the main window and press the button **Enable** near the **Trusted Applications Mode**.

3.9 Network Monitor

Network Monitor is a tool used to view information about network activities in real time. To view information about network activities, open the main application window and select the **Network Monitor** tab in the lower part of the window.

3.10 Virtual Keyboard and Secure Keyboard

Virtual Keyboard

The **Virtual Keyboard** prevents key strokes from being intercepted by keyboard spyware (keyloggers) and personal banking details and other confidential information from being transferred to cybercriminals. As on a normal keyboard, you can use the **Virtual Keyboard** to enter any text simply by pressing the corresponding buttons with your mouse arrow. The embedded technology provides reliable protection against the latest generation of applications able to scan images from the screen and against data leaks via web browsers.

In KIS 2014, when banking or payment sites are opened in the web browser, the Virtual Keyboard's quick launch element is automatically activated in the input field. Virtual Keyboard can also be launched at any time from the software's main interface.

Secure Keyboard

KIS 2014 includes a feature for the additional protection of personal data while using a physical keyboard. If you open a bank or payment website or insert a password on any web page, **Secure Keyboard** will activate automatically. The product settings allow you to select other categories of sites where the **Secure Keyboard** protection mode should be activated.

3.11 Parental Control – Improved!

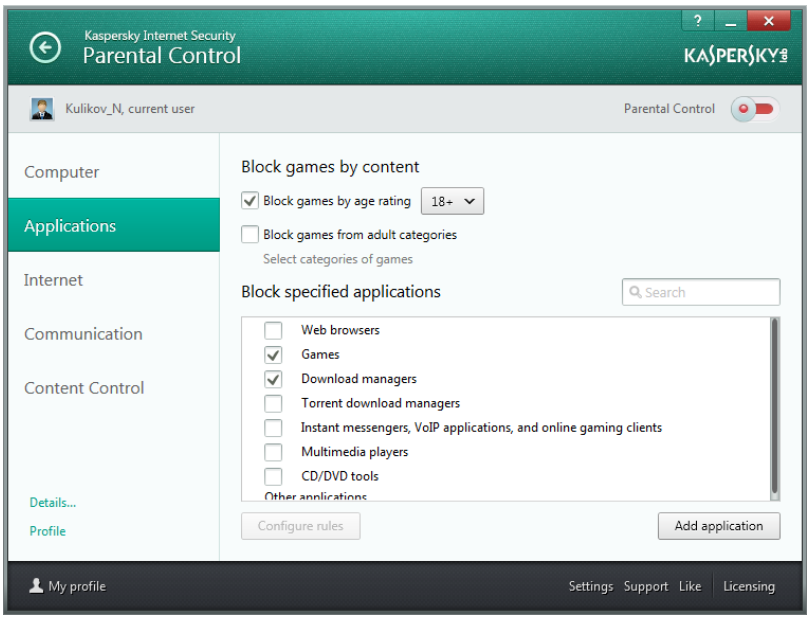
Parental Control is designed to protect children from threats on the computer and the Internet. It allows you to impose different types of restrictions:

1. Limit computer operating time.
2. Block or allow access to specific applications on the computer.
3. Block or allow access to specific websites.
4. Control your child's instant messaging (ICQ, MSN) and social networking (Facebook, etc.) communications. A complete list of instant messaging and social networking services is given below.
5. Control file downloads.
6. Control the transfer of personal information.

Parental Control supports the following instant messaging services: ICQ, QIP. MSN, Yahoo Messenger, Google Talk, mIRC, Mail.RU Agent, Psi, Miranda, AIM. Digsby, Pidgin, Qnext, SIM, Trilian, Xchat, Instantbird, RnQ, Jabber.
And the following social networks: MySpace, Twitter, Facebook.

Parental Control Improvements in KIS 2014:

1. Predefined User Profiles such as "Child", "Teenager", etc.
2. Game Rating for controlling game usage.



3. Possibility to block groups of apps, such as all games.
4. Expanded settings for controlling social networking.
5. Ability to block Internet usage by number of minutes per hour.

Social Network Control

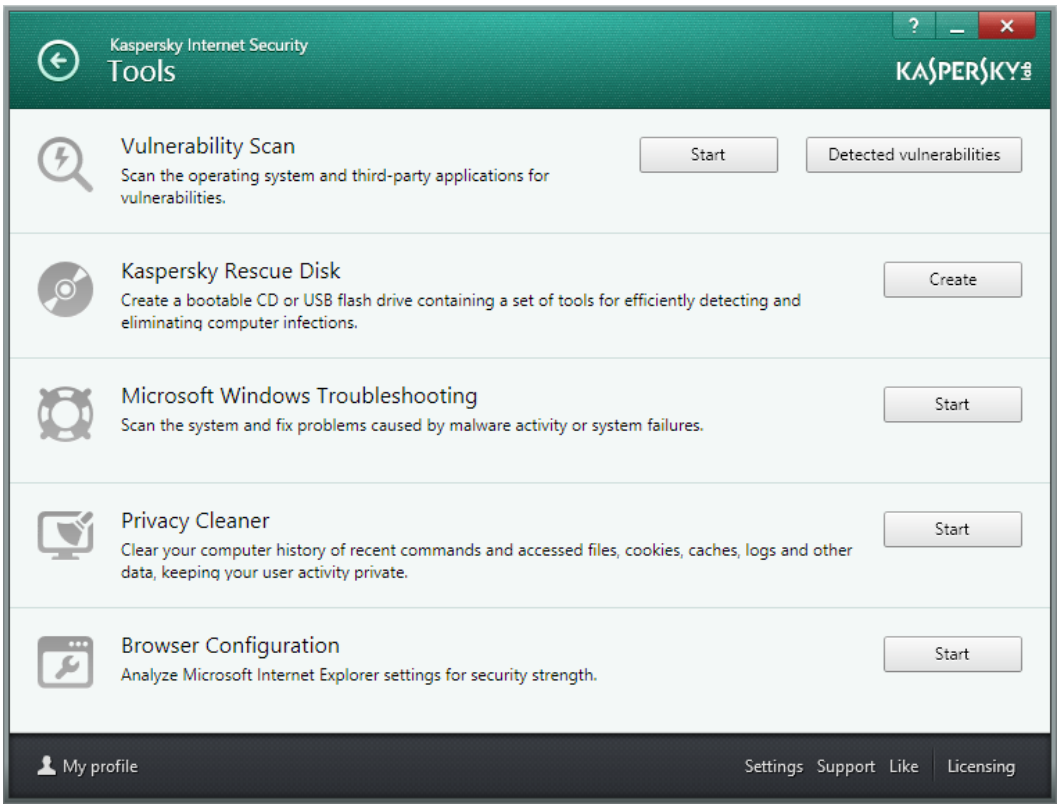
Social Network Control allows you to control your child's social networking contacts. You can block undesirable contacts and control the content of messages sent and received. You can also draw up lists of allowed and blocked contacts, set key words and phrases that will be scanned in messages, and specify personal information that cannot be sent.

3.12 Quarantine

Quarantine is a special storage area for files likely to be infected with viruses and files that cannot be disinfected as soon as they are detected. They are stored in a special format and are not dangerous to your system. Files placed in quarantine are scanned each time the antivirus databases are updated.

3.13 Tools

The Tools tab contains a set of additional tools that provide further protection for your computer.



Vulnerability Scan

A vulnerability is an error in an operating system or application that allows criminals to infect a PC without the user's knowledge. Vulnerabilities are found by examining the system, searching for anomalies or corruptions in the operating system settings, searching for vulnerable services, and other security measures.

The **Vulnerability Scan** covers all applications installed on the user's computer and matches each against one of the world's largest databases of known vulnerabilities, created and managed by Secunia, a Danish company specializing in the provision of information about critical software vulnerabilities across a range of operating systems.

To perform **Vulnerability Scan**, open **Tools/Vulnerability Scan** and press button **Start**.

Kaspersky Rescue Disk

Certain pieces of malware cause damage to the files needed to boot the operating system. In this event, you can use the **Rescue Disk**. This is a boot disk containing a set of tools to detect and cure infections on the computer in situations when the operating system and antivirus software cannot be loaded as normal.

KIS 2014 provides the option to use the product distribution disk (if the box with the product was purchased in a store) as the Rescue Disk. To do this, insert the product distribution disk in the CD/DVD drive and in the BIOS select the CD/DVD boot option. This means that you no longer need to make a rescue disk beforehand or use another computer to create one.

Microsoft Windows Troubleshooting

This wizard can help you restore the Windows operating system after it has crashed or been damaged due to a malicious attack. Our experts recommend that you disable the function to boot up automatically from flash memory in order to increase security.

Privacy Cleaner

Users always leave traces of activity, such as data entered on web forums, information about sites visited, or the names of files and folders saved on the computer.

To ensure user confidentiality, we recommend that you delete this information. This is essential, for example, if the computer is used by more than one person. The information could also be stolen over a network.

Browser Configuration

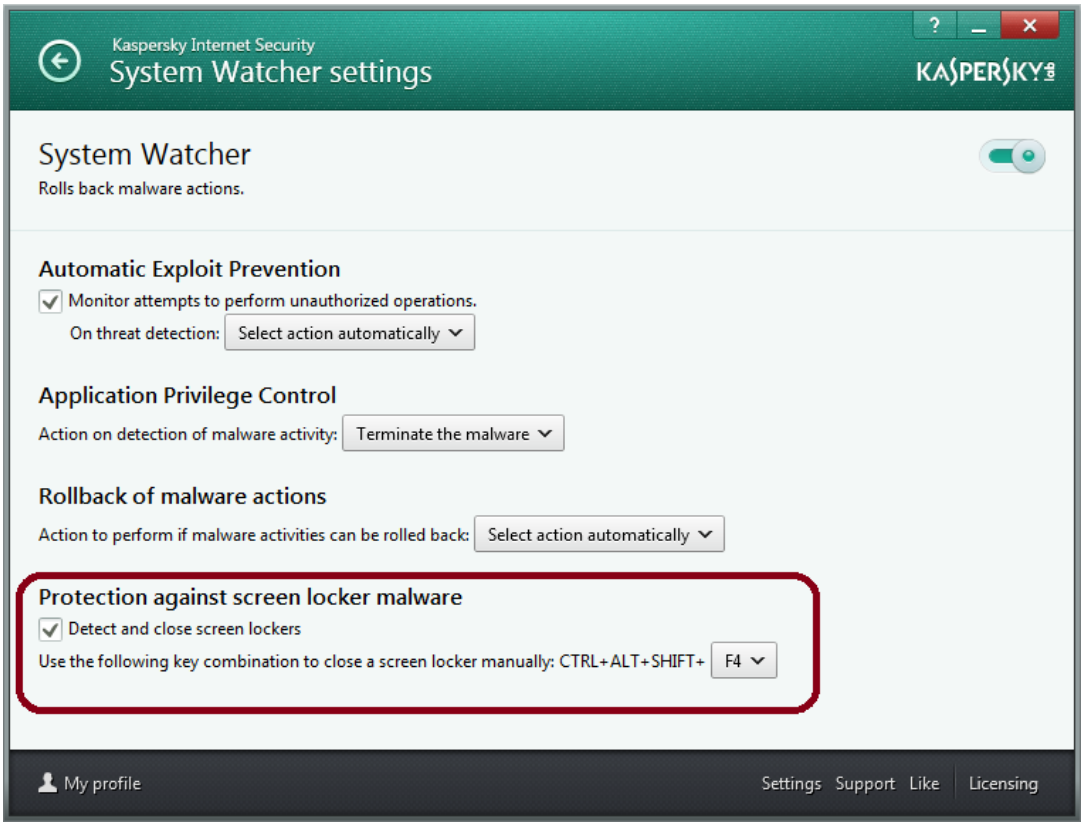
The browser configuration wizard carefully analyzes the Internet Explorer settings and suggests ways to improve them based on Kaspersky Lab's recommendations. With your consent, the settings can be changed to increase the security and protection of your confidential information when working with Internet Explorer. The changes could include, for example, blocking ActiveX components or deleting files with confidential information from the cache memory.

3.14 Anti-Blocker – new!

Blockers are Trojans that restrict access to a computer system and demand money for the restrictions to be lifted. **Anti-blocker** functionality (Protection against screen locker malware) in KAV/KIS 2014:

1. It is activated if user presses a predefined combination of hot keys, e.g., **Ctrl+Alt+Shift+F4** or if **Ctrl+Alt+Del** key combination is pressed repeatedly.
2. Next, KAV/KIS 2014 stops any dangerous processes, launches the necessary treatment procedures, records this information to Reports and sends statistics to KSN.

So, in the event a cybercriminal ever tries to control your PC with a Blocker Trojan, you can stop it in its tracks.



3.15 System Watcher

KIS 2014 includes **System Watcher**, a technology that monitors all actions performed by programs running on the computer and compares the behavior of each program with the behavioral patterns of malware. This effectively identifies new, suspicious and dangerous programs.

System Watcher also allows you to roll back malware changes.

When proactive technologies are used, it is very important to be able to roll back all actions that programs perform, if they turn out to be malicious. KIS 2014 provides this function. Depending on the product settings, rollback of malware actions is done either automatically or with your permission.

3.16 Automatic Exploit Prevention

It is common for malicious programs to exploit vulnerabilities in popular applications such as Adobe Reader, Internet Explorer, and Firefox, Java, etc. to try to gain control over the computer, steal your personal data, etc. **KIS 2014 includes Automatic Exploit Prevention technology to block the execution of such exploits.** Specifics include:

1. Control over the launch of executable files (including web browsers) if any vulnerabilities were found, or from applications which are not intended for the launch of executable files (Microsoft Word, Excel etc.).
2. If executable files are launched, their activities are checked for any signs of exploit behavior.
3. Control of any activities performed by an application where a vulnerability is detected (i.e., following the link, recording other processes to the memory, etc.). To ensure the most effective protection, all information (i.e. list of applications with detected vulnerabilities, control over the launching of executable files from applications) is updatable.

The settings can be found in the **System Watcher** settings window.

3.17 ZETA Shield

ZETA Shield technology is designed to detect malware by scanning the code of an object (file or application). The technology divides the code while it is executing on multiple data streams and analyzes these streams. The ability of ZETA Shield to work with data streams instead of individual files means it conducts more in-depth analysis of incoming data, and identifies non-standard elements, and any connections between them, to prevent the most sophisticated malware from penetrating a user's PC.

3.18 File and URL Advisors

The security status and reputation of files and websites is now at your fingertips. With a single mouse click, **File Advisor** uses cloud-based technologies to check the safety of any file you'd like to access. And our **URL Advisor** adds color-coded tags to all web links to advise you of the danger level of the link and subsequent pages. Search the web with confidence that you won't stumble onto any dangerous websites.

File Advisor

Now you can check the reputation of any file with a single mouse click. To do this, right-click on the file icon and select "**Check reputation in KSN**" (Kaspersky Security Network) in the context menu. This is handy if, for example, you have downloaded a file from the Internet, but have doubts about its safety and want to quickly check its reputation.

This function provides information about the filename, size, date created and last modified, threat rating, digital signature, geography, distribution, and other users' level of trust. All this data is displayed in Windows Explorer or in the additional section in the scan window.

The main advantage of this feature is that information from the cloud — the most up-to-date available — is used to assess the reputation of a file. This ensures that even new programs and files are safe.

URL Advisor

KIS 2014 includes the **URL Advisor** module, which informs you of links to suspicious or dangerous websites. The module is a toolbar for browsers. It flags links to infected or fraudulent (phishing) resources using a special color indicator.

URL Advisor informs you of the potential danger posed by a website before you click the link.

The process of determining danger levels utilizes not only information from the database of malicious and phishing URLs but also from the databases located on Kaspersky Lab's servers (the so-called cloud), which produce reputation scores for URLs (determined, for example, by whether or not web pages contain malicious code, how many visitors they get or whether links go to suspicious sites).

The list of supported browsers includes:

- Mozilla FireFox 16.x, 17.x, 18.x, 19.x;
- Internet Explorer 8, 9, 10;
- Google Chrome 22.x, 23.x, 24.x, 25.x, 26.x.

3.19 Settings – Improved!

KIS 2014 includes significantly optimized and reduced number of settings with the goal to leave only frequently used settings and make them more user-friendly. To view settings press link Settings in the right lower part of the program main window.

4 Licensing and support

Information about the validity period of your license can be viewed by clicking on the **Licensing** link in the lower part of the window. If you have any technical difficulties or queries about the product, you can contact our 24/7 Technical Support or use the online resources with answers to frequently asked questions on installing and using the product. Additional information on Kaspersky Internet Security 2014 technical support can be found at: http://support.kaspersky.com/