Kaspersky Lab ZAO
39A/3 Leningradskoe Shosse,
Moscow, 125212, Russian Federation

T +7 495 797-8700
www.kaspersky.com
www.securelist.com

KASPERSKY SMALL OFFICE SECURITY

(Version 3)

Features List

Contents

Overview

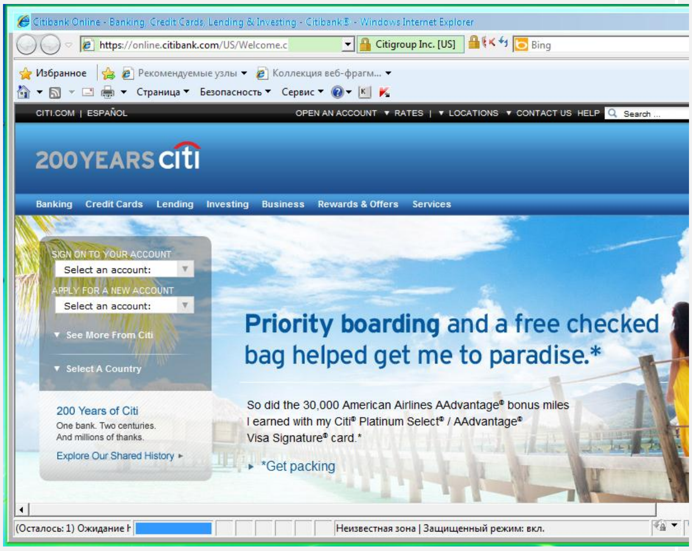
Kaspersky Small Office Security version 3 is the latest version of Kaspersky Small Office Security version. Kaspersky Small Office Security version 3 provides:

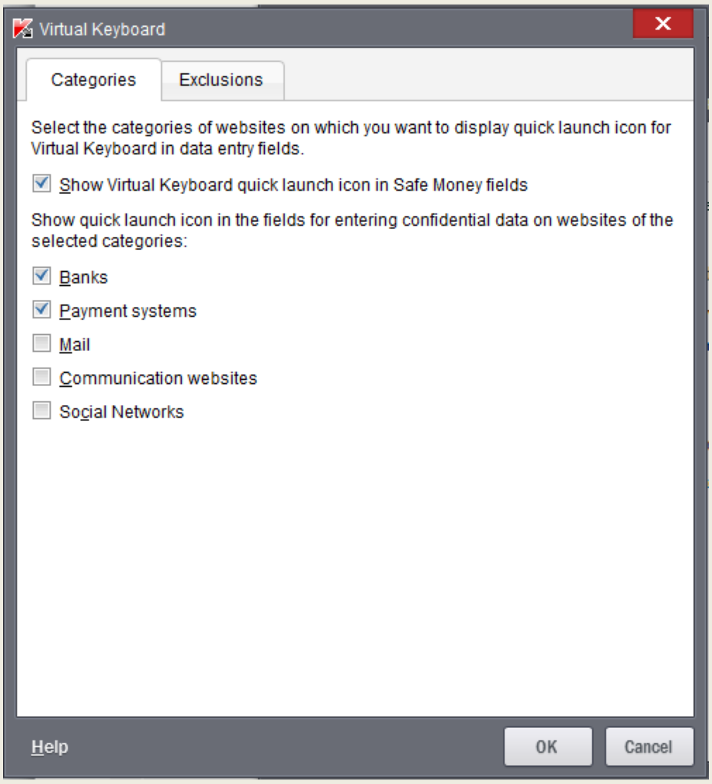
See below for detailed descriptions of each feature.

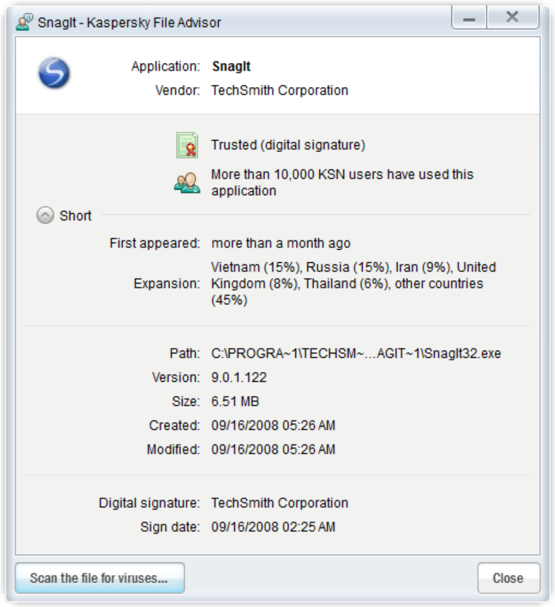
Features list for Personal Computer and File Server

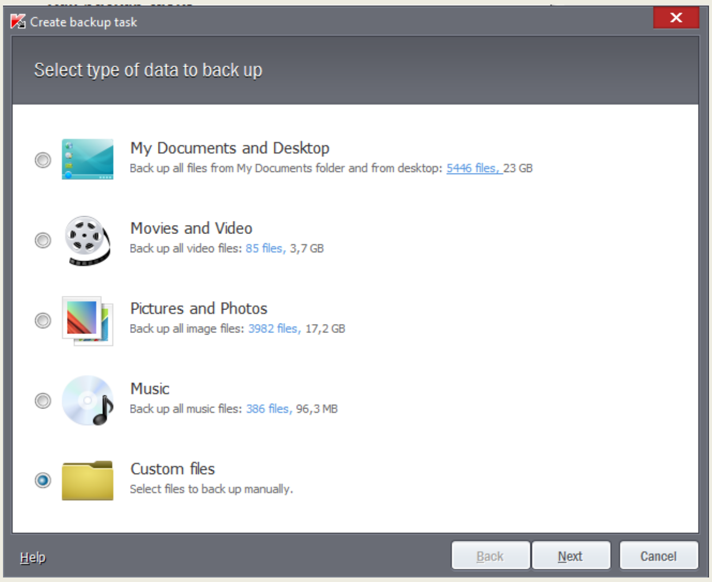
№	Feature	Features Description and User Benefits	Personal computer	File server
		Computer Security		
1	Core Protection	Kaspersky Small Office Security provides real-time protection against malware, including viruses, Trojans, worms, keyloggers, spyware and adware. The two-way personal firewall blocks hacker attacks and incoming and outgoing web traffic, emails, attachments and instant messages are all scanned for any potential threats.	■	■
2	Advanced Protection **Improved!**	Advanced proactive protection monitors system processes for suspicious behaviors using updatable heuristics modules to protect against new and unknown exploits. The Cloud-based Kaspersky Security Network (KSN) can react in 'real time' against emerging threats; as the number of threats grow exponentially, "cloud-based" proactive protection is critical to keeping your data safe. Combining cloud and proactive technologies with traditional signature-based methods provides maximum security for your computer.	■	■
3	Rootkit Detection	Rootkits usually start at boot-up; working before the operating system is launched, modifying its settings and preventing standard defenses from detecting an infection. Kaspersky Small Office Security includes dedicated anti-rootkit technology that prevents rootkits from hijacking operating system boot processes.	■	■
4	OS and Applications Control	Today's cybercriminals create malware masquerading as legitimate applications, which can seriously damage your computer and personal data. Kaspersky Small Office Security uses the latest System Watcher technology to compare a program's actions against behavioral templates. When an application tries to run on the system, Kaspersky Small Office Security confirms its security rating from our industry-leading online database and blocks any potentially dangerous applications. Even if the computer is offline, Kaspersky	■	

		Small Office Security can still apply a security rating and block a potentially dangerous application from opening. Kaspersky Small Office Security also constantly monitors any application attempting to access your private data.		
5	Rollback of malware actions	Proactive defense technologies track the behavior of programs running on the computer. If a program is malicious, you'll want to undo the actions that caused any damage. Kaspersky Small Office Security can roll back actions executed by a malicious program, even ones that occurred in the past. You can automate the rollback of malware actions and specify the amount of space (by default, 30 MB) to be set aside for logging malicious program activity on your computer.	■	■
		Internet Security		
1	Internet and Network Security **Improved!**	The Internet is the primary source of malware on users' computers, and your network is a major conduit. To keep you and your employees safe from these threats, Kaspersky Small Office Security: • scans incoming and outgoing traffic • scans websites for malicious code • checks the reputation of links before you click • detects and blocks attacks on your organization's PCs and Servers • detects and blocks phishing links that steal private and financial data • protects against spam • blocks harmful scripts • automatically modifies firewall settings according to the employees' current location (work, home or public networks for mobile workers)	■	■
2	Safe Money technology **New!**	Kaspersky Small Office Security includes Safe Money technology to protect your financial operations via online banking and payment systems (e.g., PayPal, WebMoney, etc.) and e-shops. **How it works:** Any time you enter an online banking system, bank website or payment system , Kaspersky Small Office Security: 1. Verifies that the bank or payment system website is genuine (checked against a customizable list). 2. Verifies the security certificate, avoiding possible redirection to a fake website. 3. Scans the operating system for vulnerabilities critical for online banking. 4. Recommends opening the website in Safe Money mode to further protect your personal data against	■	

		theft. When a website is opened in Safe Money mode, Kaspersky Small Office Security restricts how other programs and processes can access the site's data. When Safe Money mode is activated, a green frame will appear around the browser window indicating enhanced protection.  Priority boarding and a free checked bag helped get me to paradise.* So did the 30,000 American Airlines AAdvantage® bonus miles I earned with my Citi® Platinum Select® / AAdvantage® Visa Signature® card.* Citibank Online - Banking, Credit Cards, Lending & Investing - Citibank® - Windows Internet Explorer https://online.citibank.com/US/Welcome.c Citigroup Inc. [US] Bing Избранное Рекомендуемые узлы Коллекция веб-фрагм... Страница Безопасность Сервис CITI.COM | ESPAÑOL OPEN AN ACCOUNT RATES LOCATIONS CONTACT US HELP Search ... 200 YEARS citi Banking Credit Cards Lending Investing Business Rewards & Offers Services SIGN ON TO YOUR ACCOUNT Select an account: APPLY FOR A NEW ACCOUNT Select an account: See More From Citi Select A Country 200 Years of Citi One bank. Two centuries. And millions of thanks. Explore Our Shared History *Get packing (Осталось: 1) Ожидание h Неизвестная зона | Защищенный режим: вкл.		
3	Automatic Exploit Prevention **New!**	Malicious programs routinely exploit vulnerabilities in popular applications like Adobe Reader, Internet Explorer, Java and Firefox to try to gain control over the computer, or steal your personal data. Kaspersky Small Office Security includes a new technology, **Automatic Exploit Prevention**, that prevents and blocks these 'exploits' through: 1. Controlling the launch of executable; 2. If executable files are launched, checking their activities for any signs of exploit behavior. 3. Controlling any activities performed by an application with a vulnerability	■	■
4	Virtual Keyboard **Improved!**	The Virtual Keyboard is a secure on-screen keyboard. Entering logins, passwords, bank card details and other confidential data using the virtual keyboard keeps them safe from malicious programs that can take screenshots or record keystrokes made on a physical keyboard. Kaspersky Small Office Security now provides quick and easy access to the Virtual Keyboard from web browsers. The Virtual Keyboard is automatically activated when banking or payment sites are opened in the web browser.	■	■
5	Secure Keyboard mode **Improved!**	Kaspersky Small Office Security includes additional protection of personal data when using a physical keyboard. When you open a bank or payment website or insert a password on any web page, Secure Keyboard mode will activate automatically, creating a secure	■	■

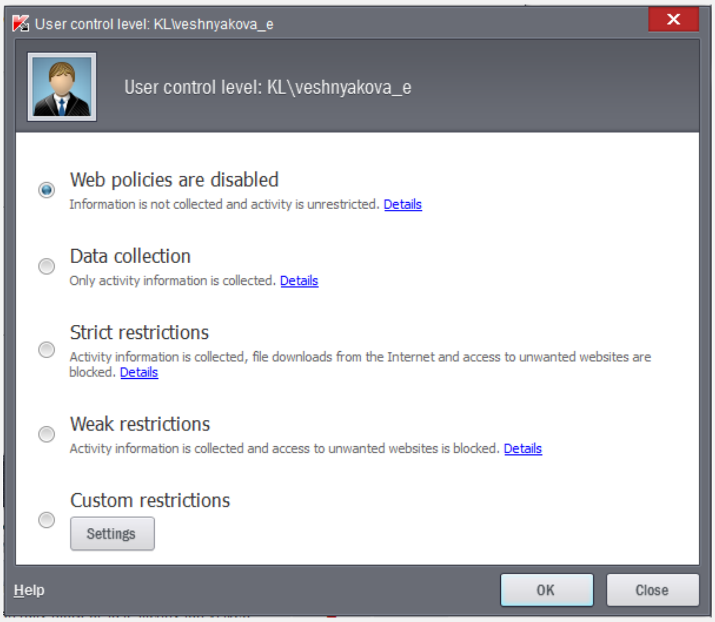
		connection between your physical keyboard and your computer. You can also select other categories where the Secure Keyboard protection should be activated.  Virtual Keyboard Categories Exclusions Select the categories of websites on which you want to display quick launch icon for Virtual Keyboard in data entry fields. ☑ Show Virtual Keyboard quick launch icon in Safe Money fields Show quick launch icon in the fields for entering confidential data on websites of the selected categories: ☑ Banks ☑ Payment systems ☐ Mail ☐ Communication websites ☐ Social Networks Help OK Cancel		
6	Anti-phishing protection **Improved!**	To access your private and financial information, cybercriminals create fake (phishing) sites. To protect you from inadvertently visiting these fraudulent websites, Kaspersky Small Office Security uses the latest heuristic analysis to check whether a URL has characteristics typical of a phishing website.	🟥	🟥
7	URL Advisor **Improved!**	Built into browser toolbars, a URL Advisor alerts the user to infected or fraudulent (phishing) sites by highlighting them in a special color which is visible in search engine results. To obtain more detailed information about a specific website, just place the cursor over the colored indicator.	🟥	🟥
9	File Advisor **Improved!**	To determine if an application you have downloaded from the Internet is going to harm your computer, simply right-click the file icon and select the context menu option: "Check reputation in KSN (Kaspersky Security Network)". Detailed information about the file will be displayed, including the level of trust assigned by other users.	🟥	🟥

		 SnagIt - Kaspersky File Advisor Application: SnagIt Vendor: TechSmith Corporation Trusted (digital signature) More than 10,000 KSN users have used this application Short First appeared: more than a month ago Expansion: Vietnam (15%), Russia (15%), Iran (9%), United Kingdom (8%), Thailand (6%), other countries (45%) Path: C:\PROGRA~1\TECHSM~...AGIT~1\SnagIt32.exe Version: 9.0.1.122 Size: 6.51 MB Created: 09/16/2008 05:26 AM Modified: 09/16/2008 05:26 AM Digital signature: TechSmith Corporation Sign date: 09/16/2008 02:25 AM Scan the file for viruses... Close		
10	Anti-Spam **Improved!**	Most Internet users have encountered irritating or dangerous spam at some point. Kaspersky Small Office Security incorporates a new and improved Anti-spam technology with even more reliable filtering of unwanted messages. Reporting on detected spam messages has been greatly enhanced.	■	
11	Anti-Banner	The Anti-Banner module blocks pop-up windows, so you don’t have to waste valuable working time getting rid of them.	■	
12	Browser compatibility **Improved!**	Many features and modules of Kaspersky Small Office Security (URL Advisor, Anti-Banner, Virtual Keyboard, Safe Money, etc.) support recent versions of the following web browsers: 1. Internet Explorer 8,9, 10 (except IE10 Metro Style UI) 2. Mozilla Firefox 18.x-22.x 3. Google Chrome24.x-28.x The product installs the appropriate plugins for a fast access to Kaspersky Small Office Security features.	■	■ (except SafeMoney)
		Backup & Restore		
1	Data backup	Nobody wants a computer crash, but sometimes it happens. To ensure the safety of your valuable information, you can easily configure your system for regular backups. Then a few simple mouse clicks can restore the system when necessary. You can use the hard drive, any removable media, an FTP server or any other network storage to store backup copies.	■	■
2	Online Backup **New!**	Kaspersky Small Office Security now integrates online backup via Dropbox – a service trusted by over 100	■	■

		million users. Free storage is based on the standard Dropbox conditions –up to 2 GB[1] free of charge. The advantages of online backup storage are: • The backup copies of files are stored in one place – a protected online storage. In case of emergency (e.g., damage to the hard drive on the PC or File Server, computer theft, etc.) your most important files will not be lost or damaged. • You can access the backup copies of your files from any computer with an Internet connection. This function requires a Dropbox account. You will be prompted to register or login when you create a backup task and choose the source "Online Storage".		
3	Data backup by category	Kaspersky Small Office Security allows you to select either the file category (audio, video, images, etc.) or the individual files you want to back up, and to decide where the backup copies should be stored.  Create backup task Select type of data to back up ○ My Documents and Desktop Back up all files from My Documents folder and from desktop: 5446 files, 23 GB ○ Movies and Video Back up all video files: 85 files, 3,7 GB ○ Pictures and Photos Back up all image files: 3982 files, 17,2 GB ○ Music Back up all music files: 386 files, 96,3 MB ● Custom files Select files to back up manually. 	🟥	🟥
4	Anywhere restore	It is possible restore backed-up data onto any computer on your network, even one without Kaspersky Small Office Security installed. Just run the standalone utility that can be added to any removable disk configured as backup storage. You can restore the whole data set, or any single file that was backed up.	🟥	🟥
5	Storage of multiple versions of files	You can choose how many file versions should be backed up. This means you can restore several previous versions of documents as required.	🟥	🟥
6	Backup tasks	You can choose when and how often backup tasks are carried out: hourly, daily, weekly, monthly, and at any	🟥	🟥

[1] Please, see Dropbox for updates.

	according to your schedule	specified time of day. Once configured, backups occur automatically at the interval you've chosen.		
7	Blocking unauthorized access to data	You can protect your backup storage with a password, restricting access to your data from unauthorized users. Each backup can be assigned an individual password.	■	■
8	Back up to network drives and FTP servers	Network drives or FTPs can also be used to back up data.	■	■
		Web Policy Management		
1	Web Policy Management	**Web Policy Management** lets you administer and monitor web policies from an administrative console–providing granular control of internet access for your users.	■	
2	Manage your organization assets usage times	Internet usage in the office can be limited flexibly, so that for example some sites may only be accessed during the lunch hour, increasing staff productivity and controlling connectivity costs. It is also very easy to block the execution of specific applications and set PC usage schedules.	■	
3	Safe Search	Popular search engines such as Google have a special **Safe Search** mode that blocks pages with inappropriate content. **The Safe Search option** in Kaspersky Small Office Security can ensure that this mode is always engaged.	■	
4	File download control by file type	Kaspersky Small Office Security can block specific file types (e.g. audio, video files) from downloading. This helps reduce Internet bandwidth usage, and helps ensure compliance with legislation.	■	
5	Supervise instant messaging communications	Employees can be limited to communicating only with specific contacts through Instant Messaging, allowing the business to enjoy the benefits of IM without time being wasted on unrelated chat. All the communications can be logged, and specific contacts white/blacklisted.	■	
6	Supervise social networking activities **New!**	People spend a lot of time on social networks, which can have a negative effect on staff productivity. Now you can supervise your employees' activity on the most popular social networks – Facebook, Myspace and Twitter - in line with your organization policy.	■	
7	Personal information	**You can prevent your employees from sending confidential information**, such as phone numbers, addresses or banking details, over the web. Simply indicate what information should be protected, and it will be blocked if any attempt is made to send the data.	■	
8	Keywords	Specific words can be added to a blacklist, and Kaspersky	■	

		Small Office Security will block data submission and notify you if those listed words were used in employee communications.		
9	Monitor all your employees PC activities	Kaspersky Small Office Security creates statistical reports on computer, applications and Internet usage, as well as IM communications.	🟥	
10	Remote policy management	All employee web surfing and usage policies can be managed by a remote administrator. For more information, refer to the details about Management Center.	🟥	
11	User-friendly settings	For simplified configuration of your company's web surfing and usage policies, the user-friendly interface has been enhanced. The administrator can simply select the desired level of restriction – choosing between pre-defined restriction levels or developing customized web policies to meet your specific needs.  User control level: KL\veshnyakova_e User control level: KL\veshnyakova_e ● Web policies are disabled Information is not collected and activity is unrestricted. Details ○ Data collection Only activity information is collected. Details ○ Strict restrictions Activity information is collected, file downloads from the Internet and access to unwanted websites are blocked. Details ○ Weak restrictions Activity information is collected and access to unwanted websites is blocked. Details ○ Custom restrictions 	🟥	
		Data Encryption		
	Secure vaults to store valuable information	You can create special, protected containers to store your commercially valuable and confidential data. Each container is encrypted and password-protected to secure your stored data against thieves and hackers. The container can be mounted as a disk on a system, and files can be copied to and from the container in just the same way as any normal hard disk.	🟥	🟥
	Securely transfer data between computers	Containers can be copied and securely transferred (via email or USB drive) between computers that have Kaspersky Small Office Security installed, carried on USB drives or sent by email.	🟥	🟥

	Create multiple vaults	You can create as many secure containers as needed, so every employee can have a secure place for his or her working data. Each container can be protected by an individual, unique password.	■	■
		Password Manager		
	Manage passwords for websites and Windows applications	Kaspersky Small Office Security helps you manage passwords for websites and applications you use within Windows.	■	
	Automatically login to websites	Kaspersky Small Office Security remembers your usernames and their associated passwords so that when you return to a site it will provide your login data automatically and securely. Password Manager also works with applications that require authentication.	■	
	Store all your passwords in a secure place	All passwords are saved in an encrypted database. Access to the password database can be locked either manually or automatically after a specified period of inactivity.	■	
	Password are accessible to employees who work out of office	The encrypted password database can be copied to a USB stick for portability. This ensures mobile employees can work seamlessly from any PC's with Kaspersky Small Office Security installed or while on the road without the added stress of remembering all of their passwords.	■	
	Master password, USB and Bluetooth authorization	Employees can control access to their password databases with a master password or by using a USB or Bluetooth device. A mobile phone can also be used as a key: passwords can be configured so that they are only available when your mobile phone is connected to your computer via Bluetooth. If the Bluetooth link is disconnected, the database will automatically lock itself.	■	
	Completes lengthy forms	An 'Identity card' created in Kaspersky Small Office Security will remember frequently used responses and complete lengthy forms automatically, saving you precious working time which adds to your profits.	■	
	Create unique and stronger passwords for better security	Kaspersky Small Office Security can generate secure, random passwords for better security. Best security practice is to have a unique password for every site or application, so the use of a single password stolen from you or your employee is limited and the risk to your data is reduced. Kaspersky Small Office Security store and enters your individual password each time – so you can use as many different passwords as you need without fear of forgetting any of them.	■	
	Import	Browsers such as Internet Explorer or Mozilla Firefox can	■	

	passwords from other applications	also store passwords, but this is in an unprotected format which can easily be accessed by cybercriminals. Password Manager helps to locate these unprotected passwords, importing them into the encrypted password database.		
	Automatically backup passwords	Kaspersky Small Office Security automatically backs up passwords each time changes are made to any account.	■	
	Encrypted Safe Notes	Password Manager now has a built-in encrypted notebook in which as user can store personal or confidential notes. This notebook can only be accessed and read if the Password Manager database is unlocked.	■	
	Protects from keyloggers and phishing	By eliminating the need to use a keyboard to enter passwords, Password Manager renders keyloggers and phishing sites useless.	■	
	Supports multiple accounts	Password Manager supports multiple accounts for shared PCs.	■	
	Supports the majority of web browsers	Supports Google Chrome (New!), Microsoft Internet Explorer and Mozilla Firefox browsers.	■	
	Removes activities history (cookies, caches, logs and etc)	Cleans up web browsing activity histories like cookies, caches, logs etc.	■	
		Additional Tools		
	File Shredder	The File Shredder wizard irreversibly wipes confidential data using multiple-pass algorithms.	■	
	PC Cleaner	The PC Cleaner wizard deletes unnecessary temporary files, log files, registry entries, browser and application caches, as well as empties the Recycle Bin.	■	
	Tune up Microsoft Internet Explorer settings for better security	Suggests optimal browser security settings to reduce risk to your company from malicious web content.	■	
	Restores system settings after removing malicious software	Removes malware from infected operating systems and restores the PC to the settings that were in place just prior to the infection.	■	
	Rescue CD for emergency renewal	A Rescue CD provides tools to clean PCs of malware and restore system settings, even if the OS was damaged. The rescue utility will try to connect to the Internet and download the latest malware database definitions to	■	

		ensure a thorough and effective cleaning process.		
	Helps secure and monitor your organization network	The security status of all the computers on your network can be seen from the manager's screen. Security problems on any computer can be fixed remotely from any other PC on the network.	■	
		Management Console		
	Centralized security management	Routine security tasks, and custom backup tasks for each computer, can all be run through the Management Center on a single PC.	■	
	Checks Wi-Fi network security	The Management Center scans the organization's Wi-Fi network, giving advice on improving security if needed.	■	
	Local virus definition update server	One computer in your network, assigned the role of update server, can download all updates from Kaspersky Lab's servers and make them available to the rest of your network, helping reduce the load on your internet bandwidth.	■	
	Remote license management	Kaspersky Small Office Security licenses for all PCs and Servers in your network are easily managed in the Management Center.	■	

Protection for Mobile Devices

Customer purchasing KSOS licenses automatically receive not just centrally managed protection for desktops, laptops and file servers, but also protection for Android based smartphones and tablets. Protection for mobile devices is provided by a KL consumer product – Kaspersky Internet Security for Android (KIS for Android) - so mobile asset protection is not managed centrally.

As KIS for Android is activated via a corporate (KSOS) license, the mobile device user will not be able to use all KPC privileges (intended for consumer products) when logging in on the KPC: only the information about the individual license will be shown.

KSOS customers benefit from all the premium features of KIS for Android.

Kaspersky Internet Security for Android – key features

	Feature	Premium
ANTIVIRUS PROTECTION	Latest protection technologies	●
	Real-time protection	●
	Automatic scan	●

	On-demand scan	●
ANTI-THEFT PROTECTION	Lock and Locate	●
	Data Wipe	●
	Alarm	●
	Mugshot	●
	SIM Watch *(available for smartphones only)*	●
	Secret code (for activating anti-theft commands)	●
	Kaspersky Anti-Theft Web Management	●
WEB PROTECTION	Blocks dangerous links while surfing websites	●
	Checks links in received text messages *(available for smartphones only)*	●
CALL & TEXT FILTERING *(available for smartphones only)*		●
PRIVACY PROTECTION *(available for smartphones only)*		●
DEVICE OPTIMIZED PERFORMANCE AND USABILITY		

Feature	Description
Antivirus Protection	
Latest protection technologies	Kaspersky Internet Security for Android delivers premium protection against viruses, spyware, Trojans, worms, bots and more. It combines traditional signature-based technologies with new proactive (i.e., heuristic) technologies, and works in the background with minimal impact on system performance. Every file, application, email attachment and media file is scanned to ensure your safety from all the latest threats. Plus, reports on all program activities – scans completed, malware found, sites blocked, and updates – are available at any time.
Real-time protection	In addition to traditional signature-based technologies and new proactive behavioral technologies, cloud security ensures maximum protection of your smartphone and tablet by providing immediate, real-time protection against new and emerging threats. • Automatic virus-scanning of downloaded applications • Immediate, real-time reaction to new and emerging threats

Automatic scan	When you purchase the software or simply activate it for a trial period, Kaspersky Internet Security for Android scans all downloaded and updated apps and files for any threats.
On-demand scan	You can manually check downloaded applications and files by running: • a full virus scan, • a folder scan, • a memory scan, • or a scan of manually installed applications.
Web Protection	
Secure Browsing	**Safe and secure web browsing** Safeguards your online identity by blocking malicious and fraudulent links, including phishing websites designed to steal your money.
Call and Text Filtering *(available for smartphones only)*	**Checking URLs within text messages** Inspects any links you receive in text messages, and notifies you whether or not they're malicious or a phishing attempt.
Anti-Theft Protection	
Kaspersky Anti-Theft Web Management	If your Android smartphone is lost or stolen, Kaspersky Anti-Theft Web Management, your personal web-based control center, provides a convenient way to remotely interact with it. Designed with simplicity in mind, the Anti-Theft Web Management portal allows you to easily: • Activate all anti-theft commands: Lock, Data Wipe, Locate, Alarm, Mugshot, and SIM Watch • Review logs of recent activities, such as commands activated, and status of anti-theft commands and their subsequent results
Lock and Locate	**Remote lock and mapping of your missing device** Smartphones and tablets are so small and lightweight that they're easy to misplace or swipe. You can remotely block them so no one will be able to access your private information. You can also create a custom message to display on your device's screen once it's blocked (e.g. to encourage a finder to return it). Moreover, you can get an approximate location of your tablet or smartphone using GPS, GSM and Wi-Fi connections and a Google Map link with your device's whereabouts.
Data Wipe	**Remove sensitive information** If you're unsure you'll be able to recover your lost or stolen device, you can remotely clean it of your personal information. Depending on your preferences and needs, the information can be wiped on several levels: • Wipe of SD card + personal Information – deletes all data from your SD memory card and erases any information about call history, Google Play account, e-mail and social networks accounts, text messages, contacts, and calendar events • Wipe of SD card + Device Reset – entails deleting all information stored in the device and on the card and returns it to the default factory settings

Alarm	**Activate an alarm to help with locating your missing device** If you can't find your tablet or phone and wonder if it's hiding somewhere nearby, you can activate the Alarm option via the Kaspersky Anti-Theft Web Management portal. Once the alarm is activated, your device will emit an alarm until you deactivate it with your secret code.
Mugshot	**Identify unauthorized users of your missing devices by secretly taking their picture** Looking for evidence that your Android smartphone or tablet has been swiped, or is being used by an unauthorized person? Kaspersky Internet Security for Android lets you get their "mugshot" by secretly taking a series of pictures of whoever is using your device, and then sending the pictures directly to your personal Kaspersky Anti-Theft Web Management account.
SIM Watch *(available for smartphones only)*	**Get in touch with your missing phone even if the SIM card has been replaced** SIM Watch helps you automatically lock a lost or stolen smartphone and reports the new phone number to you if the SIM card has been replaced.
Secret code	**Secret code to change setting** Kaspersky Internet Security for Android provides protection of the application from unauthorized un-installation. So third-party apps and other users cannot access the product without the secret code which only you know.
Call & Text Filtering *(available for smartphones only)*	
Call & Text Filtering	**Receive only the calls and texts that you want to receive** To ensure your mobile privacy, Call & Text Filtering helps you avoid unwanted calls and: • Easily add numbers of incoming calls & texts to your own White/Black lists – manually or automatically • Automatically block calls & texts from hidden and non-numeric numbers • Set appropriate filtering profiles – text messages only, calls only, text messages & calls
Privacy Protection *(available for smartphones only)*	
Privacy Protection	You can easily hide your private mobile communication from others. Privacy Protection allows you to hide contacts, incoming and outgoing calls & text messages, as well as relevant logs. For your convenience, the mode can be activated manually, automatically or remotely