Kaspersky Lab

Single Product Review

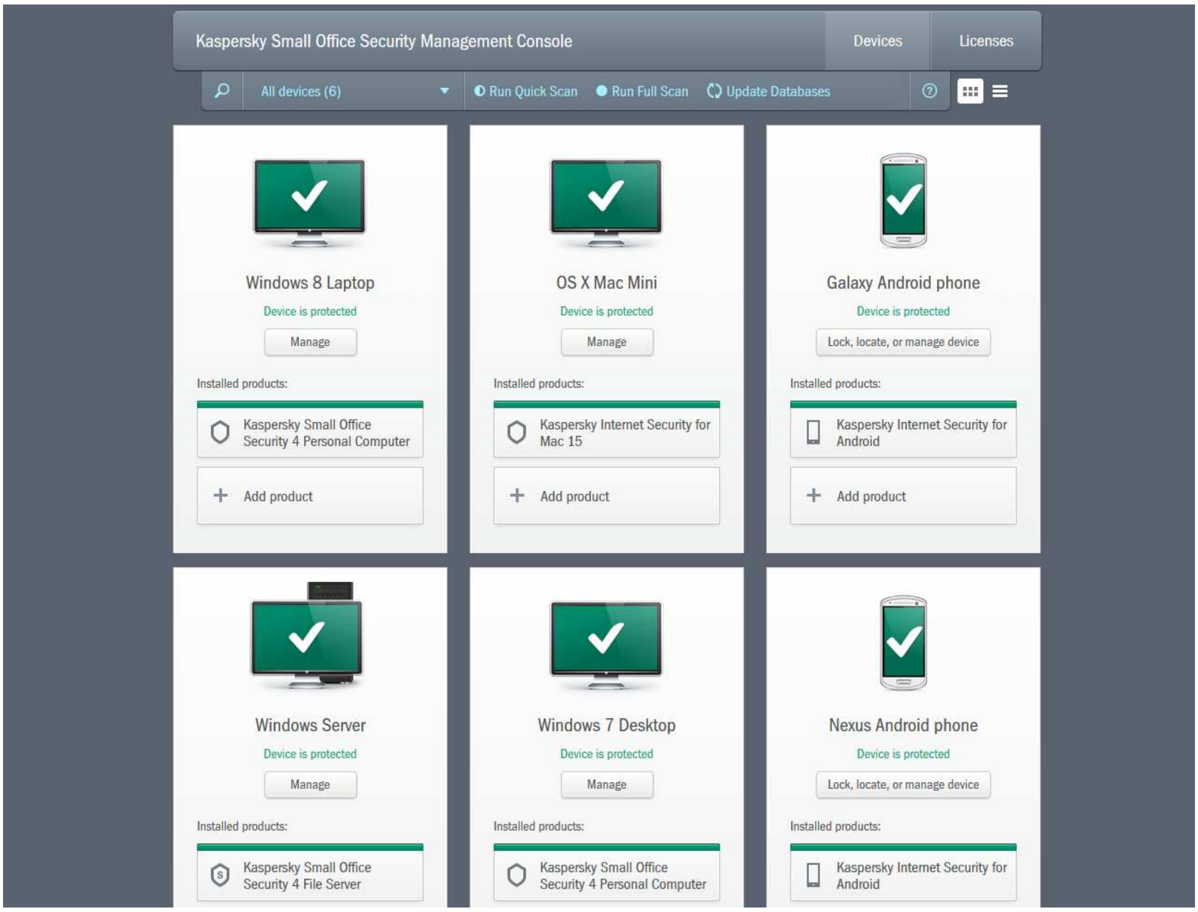
Kaspersky Small Office Security 4

Language: English
June 2015
Last Revision: 30th June 2015

www.av-comparatives.org

Test commissioned by the vendor of the product.

Introduction



Kaspersky Small Office Security 4 is a security package designed for organisations with up to 50 workstations (i.e. desktop or laptop computers). It is aimed particularly at small businesses without professional IT support, which require an easy-to-use solution that does not need a high level of technical knowledge. The suite provides protection for Windows Servers, Windows desktops and laptops, Mac OS X desktops and laptops, and Android mobile phones/tablets. All the devices can be managed via a cloud-based console; this allows administration of remote devices, not just those in the office LAN, and means that the administrator can use any Internet-connected computer or tablet, anywhere, to monitor and control protected devices.

For larger businesses, Kaspersky make two additional products: Endpoint Security for Business (in Core, Select and Advanced variants), and Total Security for Business.

Software versions reviewed

- Kaspersky Small Office Security Management Console as at June 2015
- Kaspersky Small Office Security 4 File Server 15.0.2
- Kaspersky Small Office Security 4 Personal Computer 15.0.2
- Kaspersky Internet Security for Mac 15.0.1
- Kaspersky Internet Security for Android 11.8.4

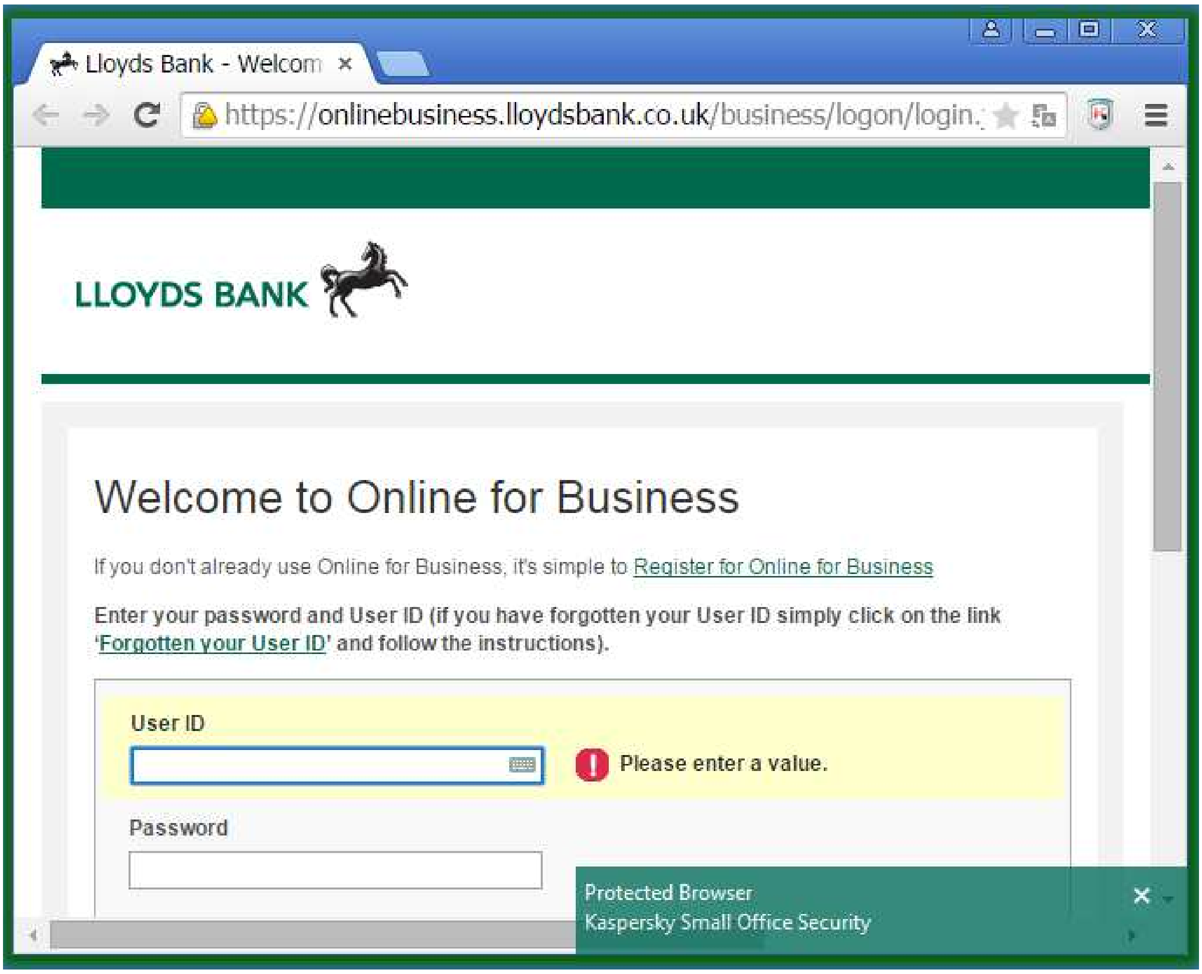
Supported operating systems

- Windows clients: Windows XP, Vista, 7, 8, 8.1, all in 32 and 64-bit versions
- Windows servers: Windows Server 2008 R2, 2012, 2012 R2; Windows Small Business Server 2008, 2011
- Mac OS X clients: OS X 10.7, 10.8, 10.9, 10.10
- Android mobile devices: Android 2.3 – 5.0

Additional features

Included in the price of the suite is *Password Manager*, a separate application that allows password management for Windows clients, Mac OS clients, Android devices and even iPhones and iPads.

In addition to the standard antimalware features, Kaspersky Small Office Security for Windows clients provides a firewall and web-usage management with download controls, both of which can be activated from the console. Other features, managed locally on the client machine, are data backup and encryption, a vulnerability scan, and *Safe Money*, which runs online transactions such as Internet banking in a specially secured browser window, indicated by a green border:



Lloyds Bank - Welcom
https://onlinebusiness.lloydsbank.co.uk/business/logon/login.
LLOYDS BANK

Welcome to Online for Business

If you don't already use Online for Business, it's simple to Register for Online for Business

Enter your password and User ID (if you have forgotten your User ID simply click on the link 'Forgotten your User ID' and follow the instructions).

User ID

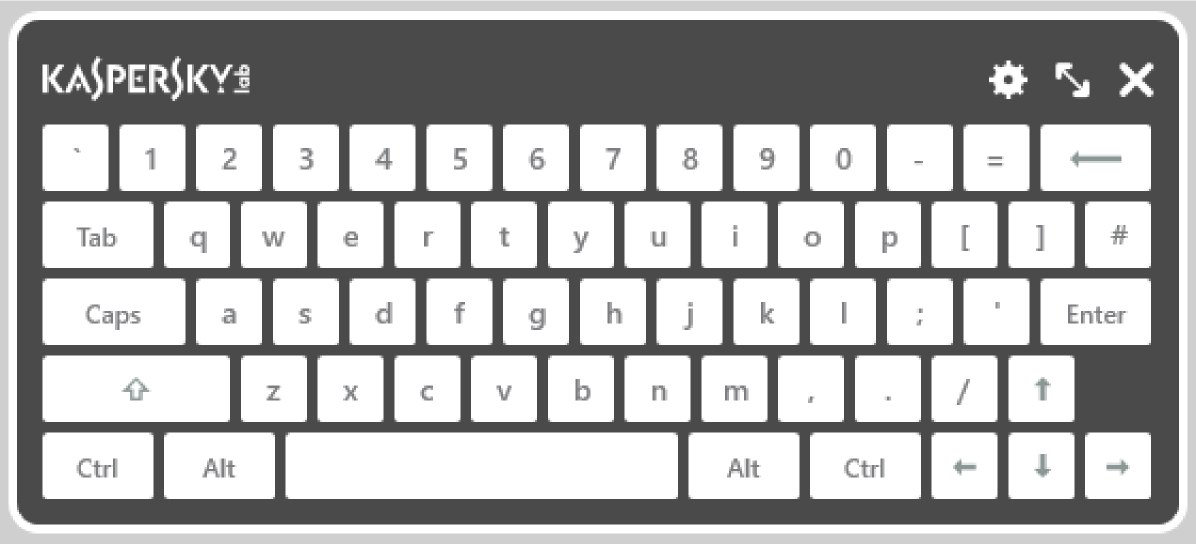
Please enter a value.

Password

Protected Browser
Kaspersky Small Office Security

The Mac client software, Kaspersky Internet Security for Mac, also includes web usage/download controls and *Safe Money*. Both of these have to be configured locally on the client machine.

The client software for both Windows and Mac includes a virtual keyboard, which enables safe input of e.g. passwords without any risk of the data being picked up by a keylogger:



Kaspersky Internet Security for Android has the console-controlled anti-theft features lock and locate, alarm, wipe, and *Mugshot*, which takes a picture of the phone's finder/thief if it is lost or stolen.

Documentation

In this section, we look at help facilities that can be accessed independently of the console or any of the software products (i.e. website and downloadable documents). Details of integrated help features can be found in the respective reports of the console and individual device protection products below.

Manuals

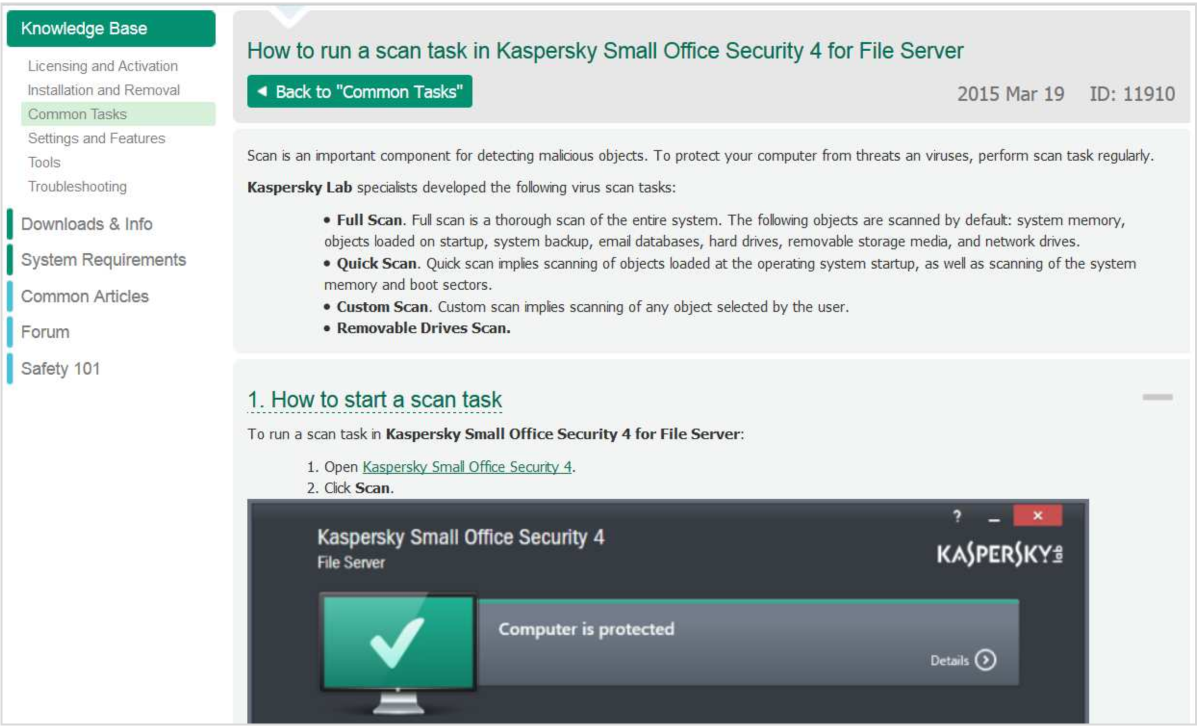
Manuals for each of the individual protection products (for Windows, Mac and Android) can be downloaded from a single page of the Kaspersky website[1]. The guide to the Windows product is 119 pages long and very detailed. It provides comprehensive instructions, with some screenshots, for installing, configuring and using the protection software for Windows server and client systems. It is written from a point of view of local management, although there are instructions for registering the software in the console so that it can be managed remotely. There is a 66-page manual with text instructions for Kaspersky Internet Security for Mac, with comprehensive text instructions, although no screenshots aside from a few icons. The document only covers local management, and does not make any reference to the console. A 52-page illustrated manual for Kaspersky Internet Security for Android is also provided, covering the installation, configuration and use of the product. Although it mentions adding a device to a web management account, this relates to a different management console[2].

[1] http://www.kaspersky.co.uk/documentation/small-office-security

[2] https://anti-theft.kaspersky.com

Knowledge base

The suite's knowledge base section on the Kaspersky Lab website[3] has very clear, well-illustrated instructions for common tasks in each of the suite's client protection products. An example page for the Windows server software is shown below:



How to run a scan task in Kaspersky Small Office Security 4 for File Server

2015 Mar 19 ID: 11910

Scan is an important component for detecting malicious objects. To protect your computer from threats an viruses, perform scan task regularly.

Kaspersky Lab specialists developed the following virus scan tasks:

- **Full Scan**. Full scan is a thorough scan of the entire system. The following objects are scanned by default: system memory, objects loaded on startup, system backup, email databases, hard drives, removable storage media, and network drives.
- **Quick Scan**. Quick scan implies scanning of objects loaded at the operating system startup, as well as scanning of the system memory and boot sectors.
- **Custom Scan**. Custom scan implies scanning of any object selected by the user.
- **Removable Drives Scan.**

1. How to start a scan task

To run a scan task in **Kaspersky Small Office Security 4 for File Server**:

1. Open Kaspersky Small Office Security 4.
2. Click **Scan**.

We could not find any Knowledge Base articles relating to remote management of the Windows or Mac software. The Knowledge Base does include instructions for remote management of Android devices, via the consumer-oriented *My Kaspersky* portal; please see our comments on possible confusion between this and the business console below.

Comment

Although the documentation for KSOS is extensive and mostly well produced, we feel that it has not been updated properly with regard to connecting and managing Mac OS X and Android devices. We suggest that the individual manuals for the Mac OS X software and Android software should both include relevant instructions for connecting to the new business console. We also feel that a separate, downloadable manual and/or Knowledge Base article for the management console, covering management of all three operating systems, would be helpful.

[3] http://support.kaspersky.com/#s_tab2

Management Console

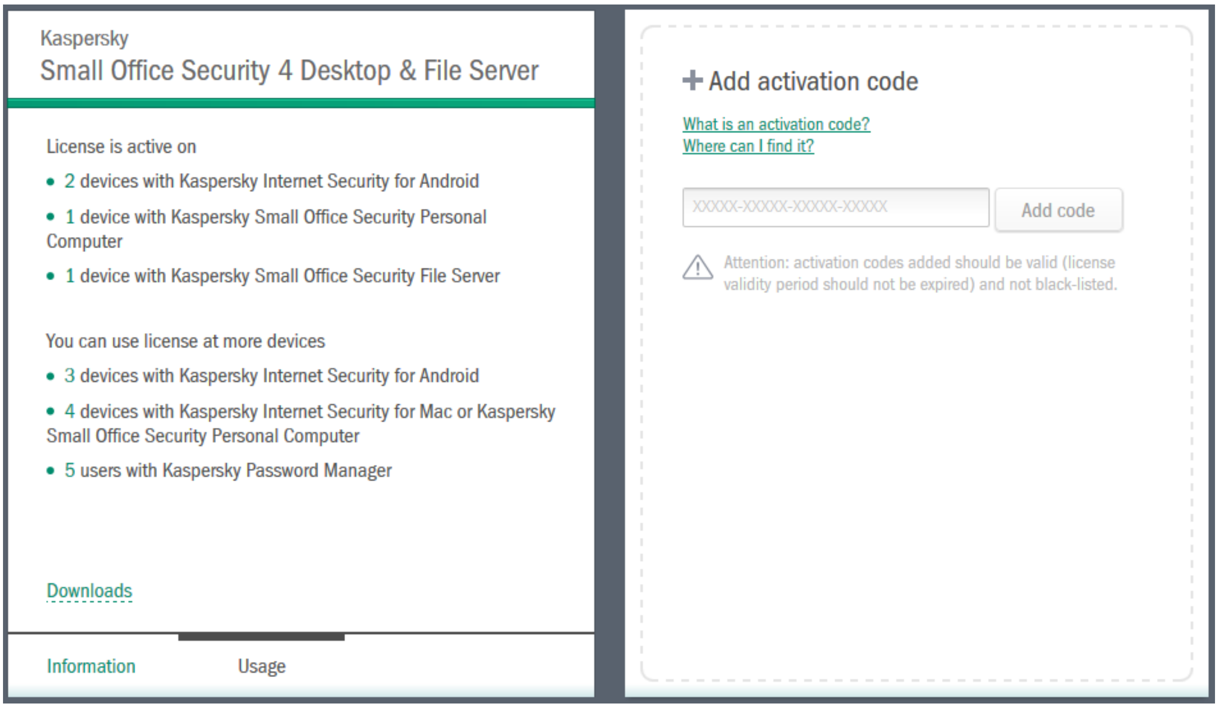
Installation and configuration

The console is cloud-based, meaning that there is no installation required. The administrator simply has to create a Kaspersky Account (a very quick process requiring a minimum of information) and log in. The web address is very simple to remember: *center.kaspersky.com*.

The instructions we received from Kaspersky Lab regarding the licence informed us that we needed to use the *Convert* button in the console, which we did. The reason for this – managing all devices from one account – was not clear, and we feel that this could be explained better. Related to this is possible confusion between the URL used for managing consumer products – mentioned in some documentation for the component products – which is https://my.kaspersky.com, and the URL for managing business products, which is https://center.kaspersky.com.

Layout

The console has two main pages, *Devices* (shown by default) and *Licenses*. The administrator can switch between the pages using the two big buttons at the top. The *Usage* view of the *Licences* page shows the number of licences being used, and how many are still available; there is also a convenient link to the *Downloads* page, from which client protection software can be installed:



Kaspersky
Small Office Security 4 Desktop & File Server

License is active on

- 2 devices with Kaspersky Internet Security for Android
- 1 device with Kaspersky Small Office Security Personal Computer
- 1 device with Kaspersky Small Office Security File Server

You can use license at more devices

- 3 devices with Kaspersky Internet Security for Android
- 4 devices with Kaspersky Internet Security for Mac or Kaspersky Small Office Security Personal Computer
- 5 users with Kaspersky Password Manager

Downloads

Information Usage

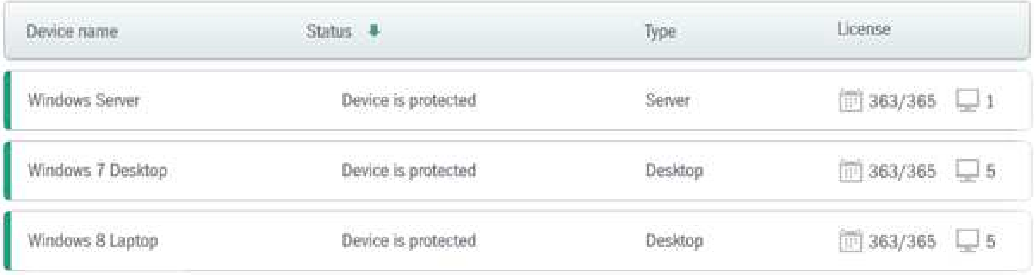
+ Add activation code

What is an activation code?
Where can I find it?

XXXXX-XXXXX-XXXXX-XXXXX Add code

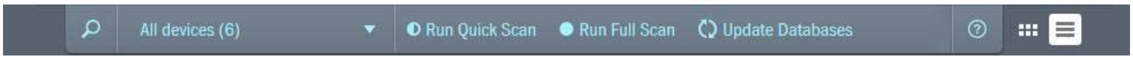
Attention: activation codes added should be valid (license validity period should not be expired) and not black-listed.

The *Devices* page displays all the protected devices. These can be shown as tiles, with detailed information (as shown in the main screenshot at the start of this report), or in the form of a list, as shown below:



Device name	Status	Type	License
Windows Server	Device is protected	Server	363/365 1
Windows 7 Desktop	Device is protected	Desktop	363/365 5
Windows 8 Laptop	Device is protected	Desktop	363/365 5

A menu bar at the top of the page allows the administrator to toggle between these two views, filter the devices shown, carry out common tasks such as scans and updates, and open the help feature:



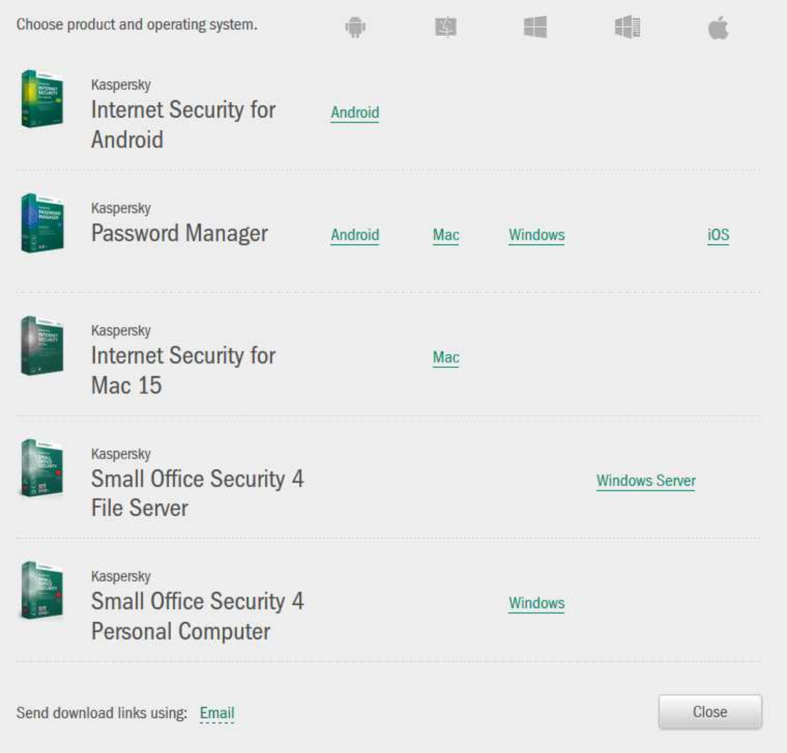
Each device is automatically assigned a name when it is installed. The administrator can easily change the display name in the console, however, simply by clicking on it and typing. We liked this, as it enables the administrator to give names that easily identify each device.

Preparing devices for deployment

No specific preparations are needed on any compatible device, other than removing any existing security software.

Deploying the endpoint protection software

To deploy protection software to devices, the administrator opens the *Downloads* page, which displays links for all the available products:



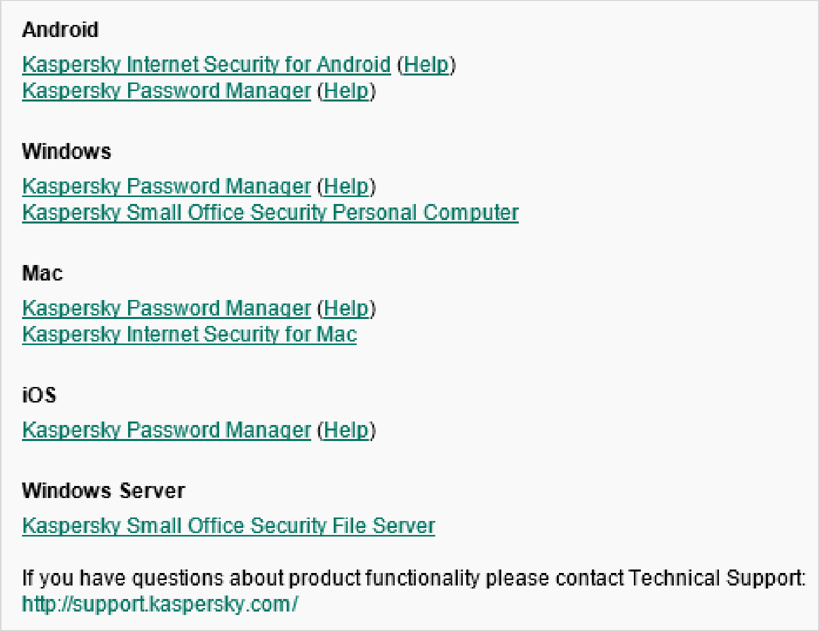
Choose product and operating system.					
Kaspersky Internet Security for Android	Android				
Kaspersky Password Manager	Android	Mac	Windows		iOS
Kaspersky Internet Security for Mac 15		Mac			
Kaspersky Small Office Security 4 File Server				Windows Server	
Kaspersky Small Office Security 4 Personal Computer			Windows		

Send download links using: Email

To install the software on the device being used to view the console, the administrator simply clicks the relevant link for the OS/product required. For Windows servers and desktops/laptops, and Mac OS X desktops/laptops, this downloads an installer file (.EXE for Windows, .DMG for Mac). The installer is then run on the local machine; details for each OS are given in the respective sections on client protection software below. For Android devices, clicking the link opens the Google Play Store at the installation page for Kaspersky Internet Security for Android.

To install software on a different computer (server/desktop/laptop), the administrator has two options. Firstly, the downloaded installation file can be copied to a flash drive and so run on any other computer – this is probably the quickest option for installing a number of computers in the same physical office. We note that there is a single installer file for the Windows software, which can be used to install the protection software on the server and clients; the setup wizard recognises the operating system and configures the product accordingly.

For remote users, the administrator can email a link with which they can download and install the software themselves. This is done very conveniently by clicking the *Email* link at the bottom of the *Download* page, typing in the relevant email address, and clicking *Send*. The user will then receive an email which includes the following content:



Android
Kaspersky Internet Security for Android (Help)
Kaspersky Password Manager (Help)

Windows
Kaspersky Password Manager (Help)
Kaspersky Small Office Security Personal Computer

Mac
Kaspersky Password Manager (Help)
Kaspersky Internet Security for Mac

iOS
Kaspersky Password Manager (Help)

Windows Server
Kaspersky Small Office Security File Server

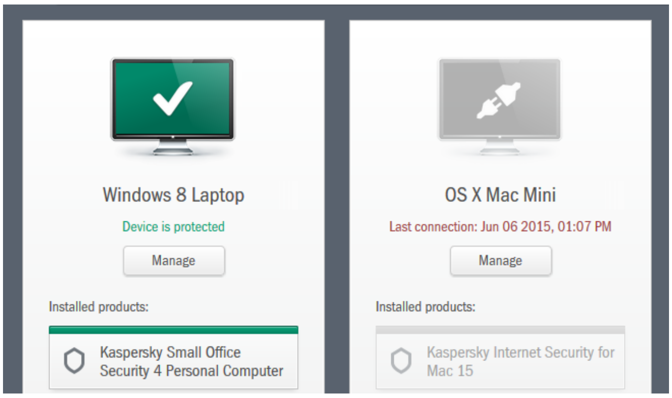
If you have questions about product functionality please contact Technical Support:
http://support.kaspersky.com/

We note that the web address of Kaspersky Lab's support service is also provided, in case the user needs assistance with installing the product.

Monitoring the network

Status

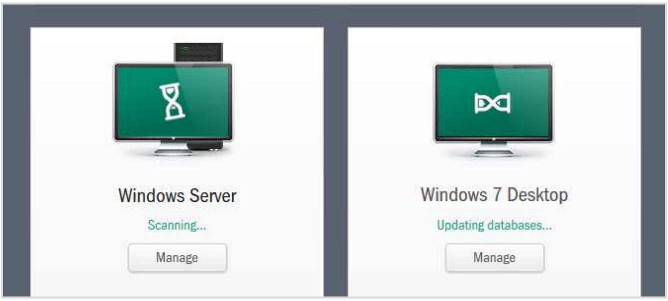
The *Devices* view of the console gives a simple, at-a-glance view of the status of the company's devices. For each device, there is an icon and caption which serve as the status display, while the Kaspersky Lab product(s) installed is/are shown in a box below If a device is protected and all is well, its icon is shown in green, with the caption *Device is protected*; devices not currently connected are shown greyed out, with the date and time of last connection to the console:



Windows 8 Laptop
Device is protected
Manage
Installed products:
Kaspersky Small Office Security 4 Personal Computer

OS X Mac Mini
Last connection: Jun 06 2015, 01:07 PM
Manage
Installed products:
Kaspersky Internet Security for Mac 15

If a scanning or updating task is being run, this is indicated by an hour glass in the computer screen of the device's icon, with the type of task shown as the annotation:

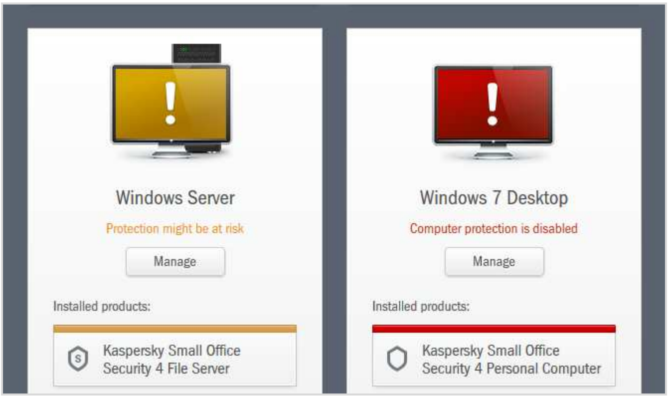


Windows Server
Scanning...
Manage

Windows 7 Desktop
Updating databases...
Manage

Warnings

Warnings are shown very clearly by the icon and its caption. To demonstrate this, we downloaded the AMTSO PUA test file on our Windows server, and disabled the real-time protection on a Windows desktop PC. The following warnings were shown:

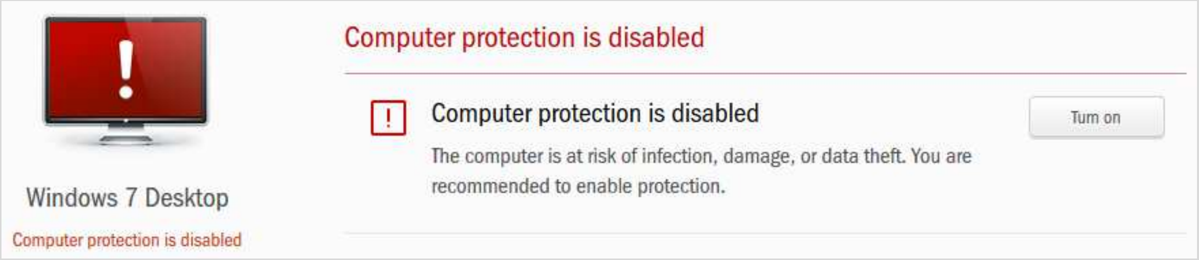


Windows Server
Protection might be at risk
Manage
Installed products:
Kaspersky Small Office Security 4 File Server

Windows 7 Desktop
Computer protection is disabled
Manage
Installed products:
Kaspersky Small Office Security 4 Personal Computer

Rectifying problems

To correct a problem shown for any device – Windows, Mac or Android – the administrator clicks *Manage*; this opens the device's details page, which provides a more detailed explanation, a recommended course of action, and the means to carry this out. The details page for the PC with disabled protection is shown below. Simply clicking the *Turn on* button reactivates the protection.



Computer protection is disabled

Computer protection is disabled

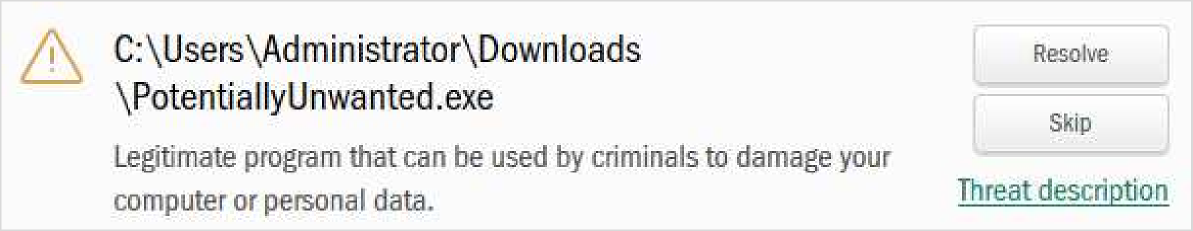
The computer is at risk of infection, damage, or data theft. You are recommended to enable protection.

Windows 7 Desktop

Computer protection is disabled

Malware alerts

If Kaspersky Small Office Security endpoint protection software detects and completely eliminates a threat, as it does with the EICAR test file, no warning is shown in the console, as no action is required of the administrator. In the case of a potentially unwanted application (PUA), a warning is shown – as illustrated by the icon for our Windows server above. This enables the administrator to decide what to do with the program:



C:\Users\Administrator\Downloads \PotentiallyUnwanted.exe

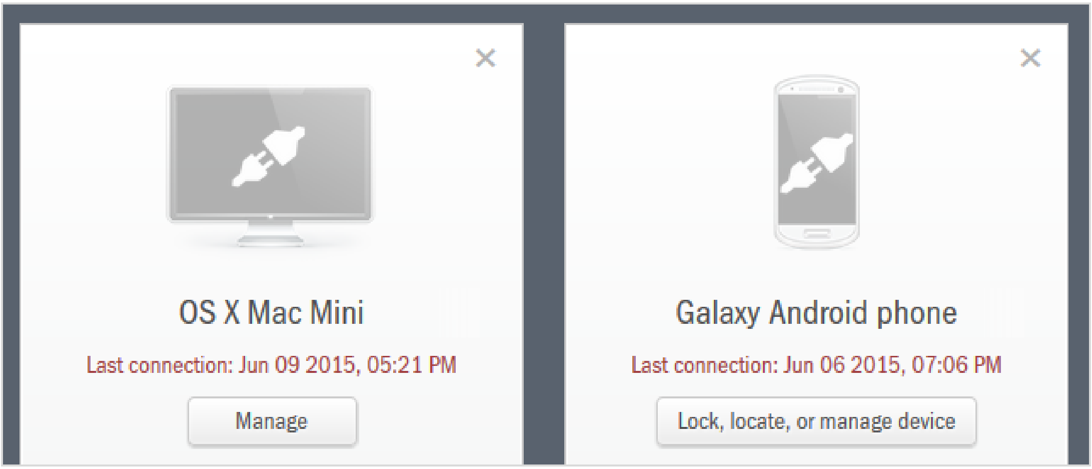
Legitimate program that can be used by criminals to damage your computer or personal data.

Program version

Whilst every device's tile shows the Kaspersky Lab product(s) installed, the administrator has to check the device locally to determine the exact program version.

Removing devices from the console

If a device has been inactive (not communicated with the console) for 4 days, an *X* symbol appears in the top right-hand corner of its tile; clicking this allows the device to be hidden from the console. This has to be confirmed, to prevent it happening by accident.



OS X Mac Mini

Last connection: Jun 09 2015, 05:21 PM

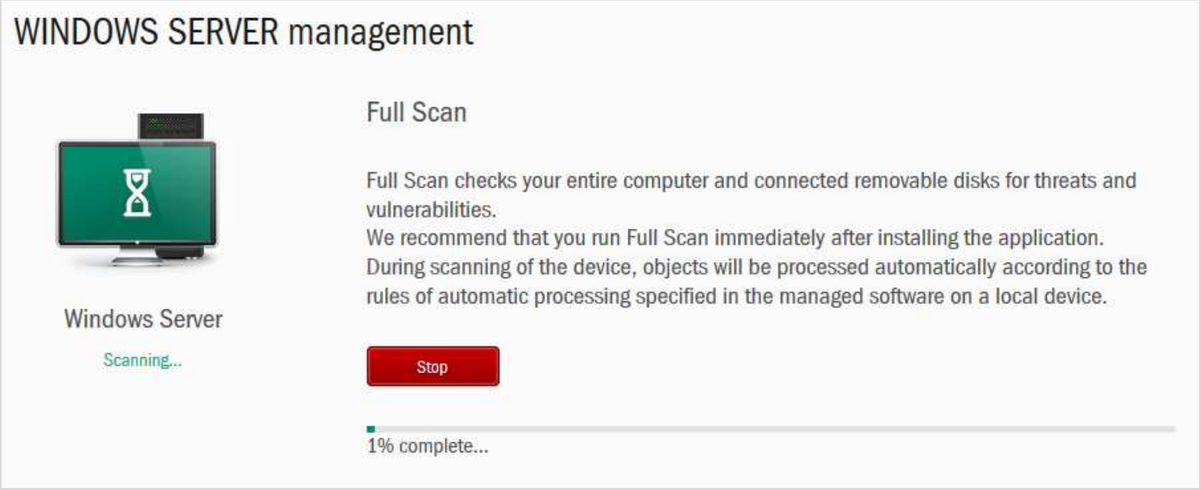
Galaxy Android phone

Last connection: Jun 06 2015, 07:06 PM

Managing the network

Scanning

To run a scan on all the devices on the network, the administrator simply clicks *Run Quick Scan* or *Run Full Scan*, as appropriate, on the *Devices* page of the console. This executes the command immediately on all devices currently connected; for devices that are offline, the scan will be run when they next connect (assuming that this is within the following 7 days). To scan an individual device, the administrator clicks the *Manage* button for that device, then *Quick Scan* or *Full Scan*, as appropriate, on the device's management page. It is possible to stop a scan from the management console – a *Stop* button appears (as shown below). We note that we had to enter the console administration password to do this.



WINDOWS SERVER management

Full Scan

Full Scan checks your entire computer and connected removable disks for threats and vulnerabilities.
We recommend that you run Full Scan immediately after installing the application.
During scanning of the device, objects will be processed automatically according to the rules of automatic processing specified in the managed software on a local device.

Scheduling Scans

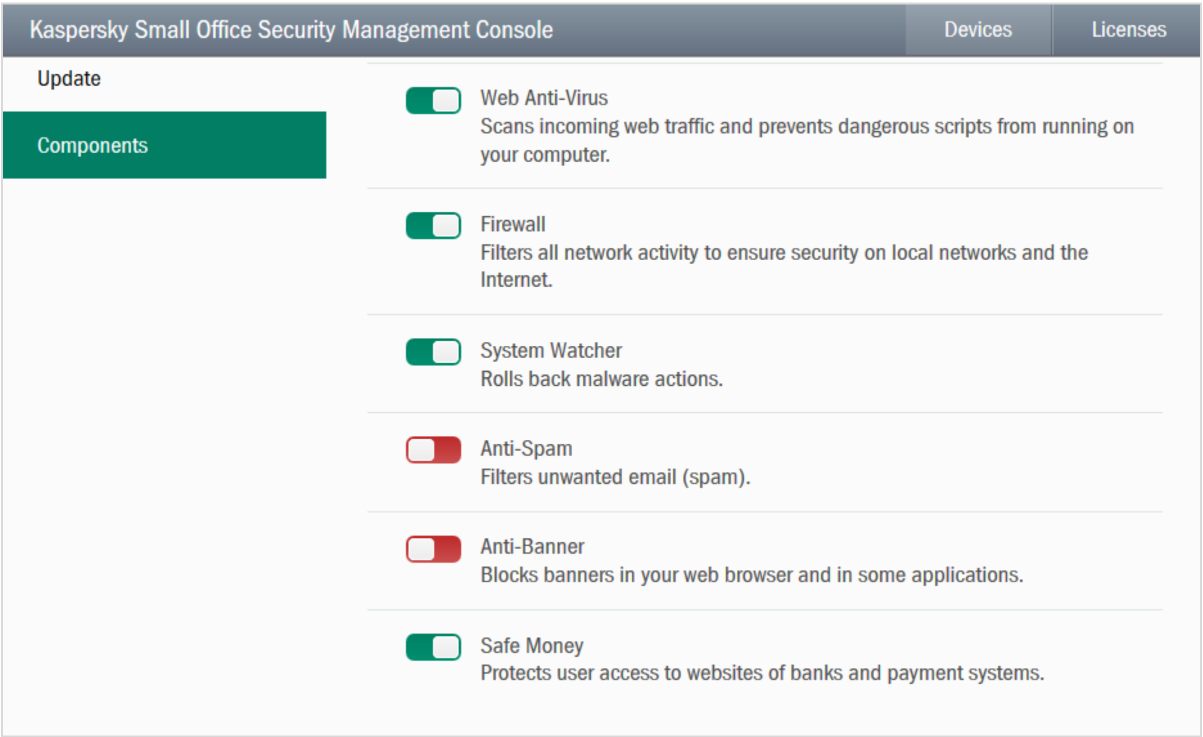
It is not possible to set a scanning schedule from the console, but this can be done on the individual PC/Server.

Updates

The process for running updates is exactly parallel to running a scan, both for all devices or just one, using the relevant *Update* button.

Components

For every computer running Windows or Mac OS X, the management page contains a link named *Components*. This allows the administrator to activate or deactivate individual protection features as necessary:



Web Anti-Virus
Scans incoming web traffic and prevents dangerous scripts from running on your computer.

Firewall
Filters all network activity to ensure security on local networks and the Internet.

System Watcher
Rolls back malware actions.

Anti-Spam
Filters unwanted email (spam).

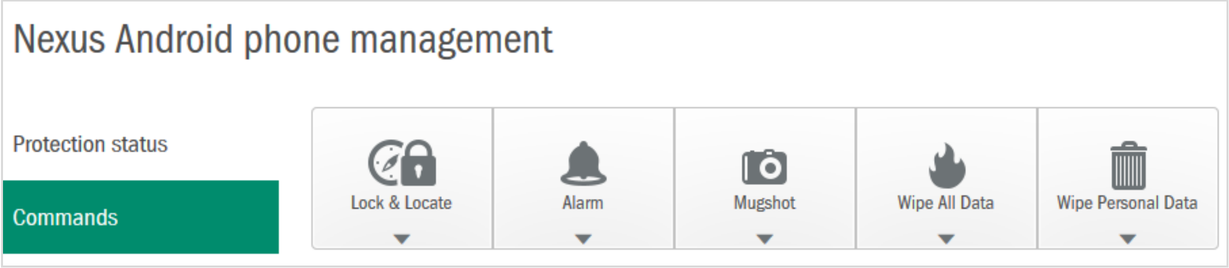
Anti-Banner
Blocks banners in your web browser and in some applications.

Safe Money
Protects user access to websites of banks and payment systems.

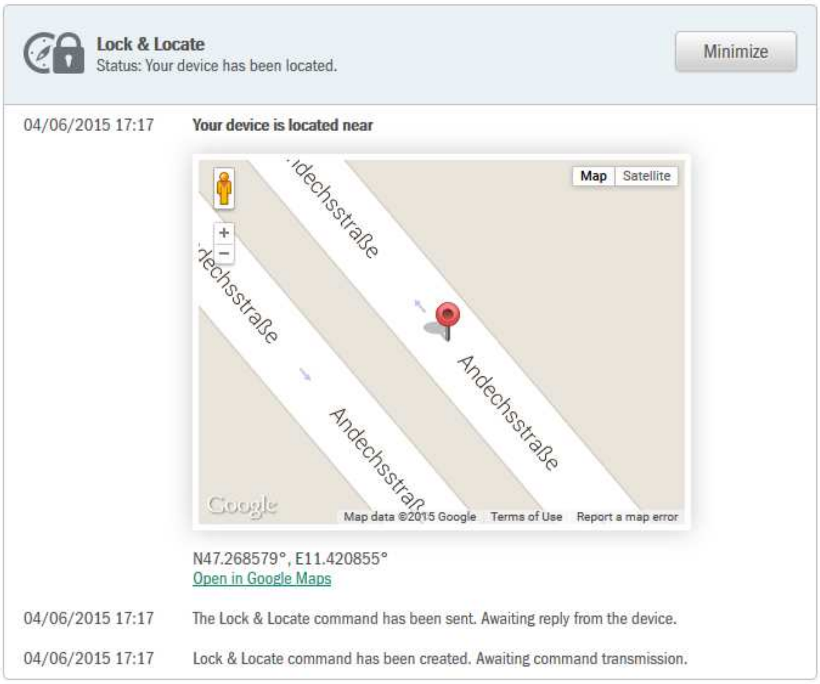
The list of components shown in the management console is tailored to the specific operating system, i.e. Windows client, Windows server, or Mac OS.

Android theft-protection management

To use the theft-protection features for Android mobile devices, the administrator clicks *Manage* for the device in question, and then either *Commands* or *Lost your device?* The available functions are then displayed:



A command can be carried out simply by clicking the appropriate icon and a confirmation. Both the *Alarm* and *Mugshot* commands lock the device, and along with *Lock and Locate* they give the administrator the chance to display a message on the screen. In our test of the *Lock & Locate* feature, the device was successfully locked and its location very accurately determined.



Status: Your device has been located.

04/06/2015 17:17 Your device is located near

N47.268579°, E11.420855°

04/06/2015 17:17 The Lock & Locate command has been sent. Awaiting reply from the device.

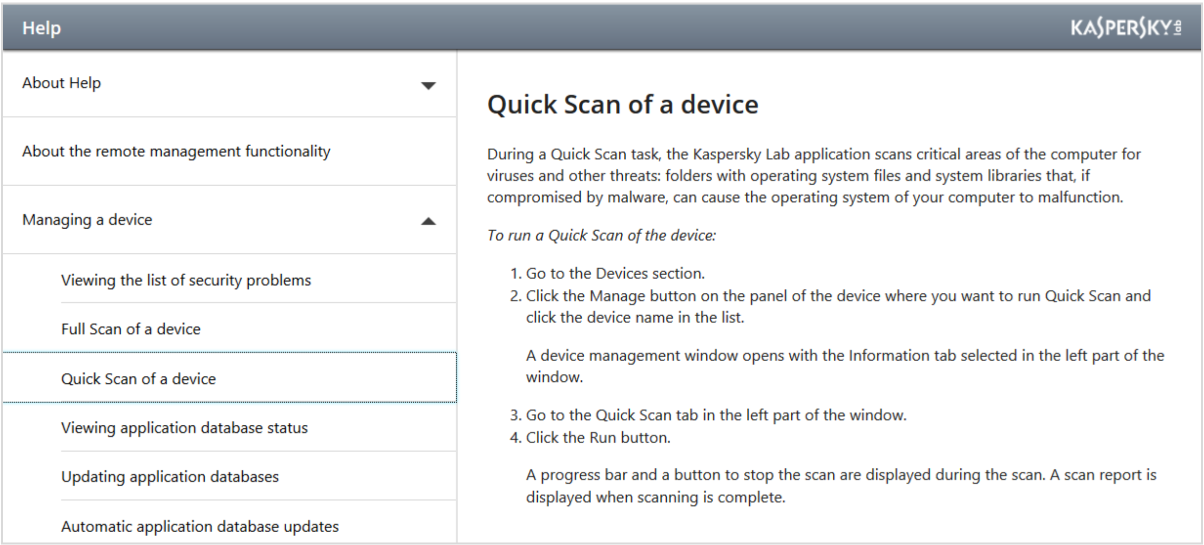
04/06/2015 17:17 Lock & Locate command has been created. Awaiting command transmission.

We also tested the *Alarm*, *Mugshot* and *Wipe All Data* (= carry out a factory reset) functions, and all worked exactly as expected.

We received emails from Kaspersky Lab stating the position of the test smartphone, and confirming that the Mugshot command had been used. In each case, the email was received within about two minutes of the command being sent.

Integrated help feature

Clicking the *?* symbol in the top right-hand corner of the console opens the help pages in a new tab of the browser. These provide a clear overview of main topics on the left, with instructions for each topic on the right. We note that the layout is very tablet-friendly, with the topics list easy to tap with a finger, and very concise instructions that can be displayed in a legible size on a small tablet screen without too much scrolling being required.


Help
KASPERSKY
About Help
About the remote management functionality
Managing a device
Viewing the list of security problems
Full Scan of a device
Quick Scan of a device
Viewing application database status
Updating application databases
Automatic application database updates

Quick Scan of a device

During a Quick Scan task, the Kaspersky Lab application scans critical areas of the computer for viruses and other threats: folders with operating system files and system libraries that, if compromised by malware, can cause the operating system of your computer to malfunction.

To run a Quick Scan of the device:

1. Go to the Devices section.
2. Click the Manage button on the panel of the device where you want to run Quick Scan and click the device name in the list.

   A device management window opens with the Information tab selected in the left part of the window.

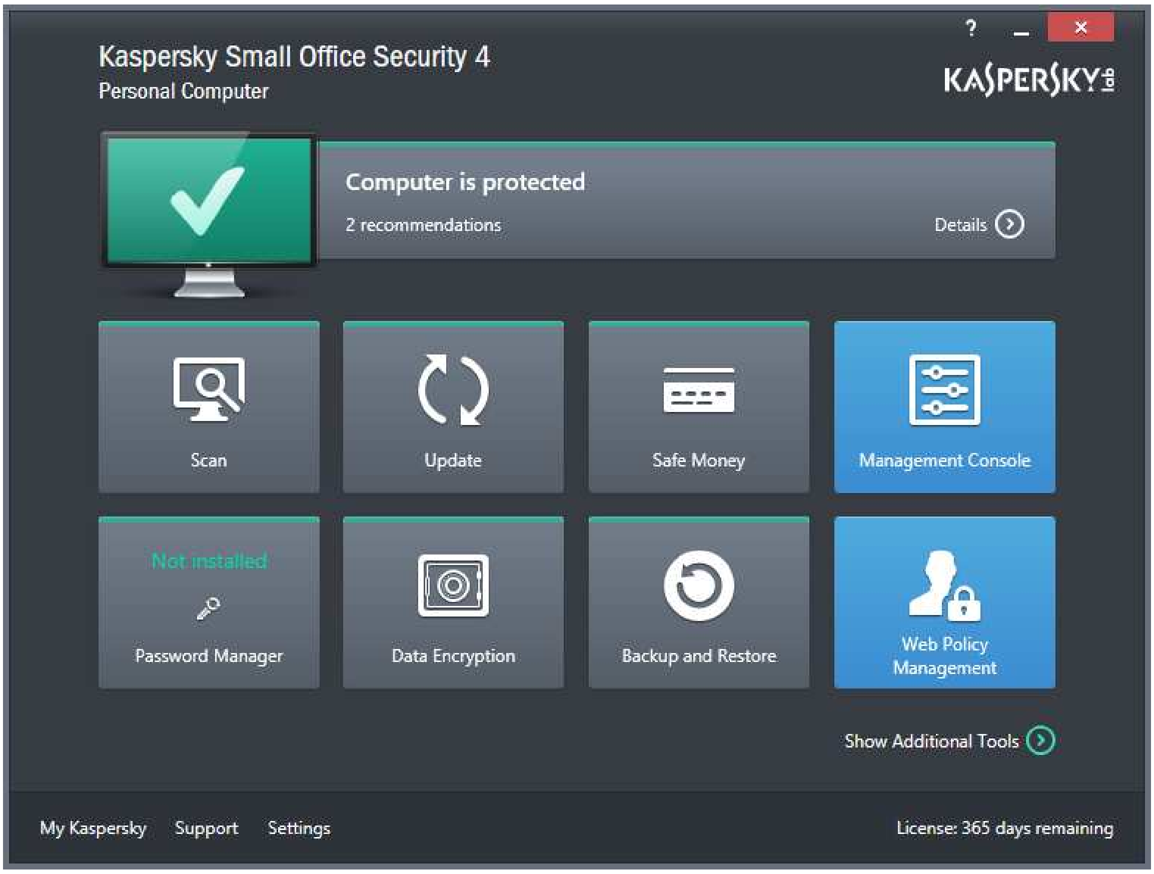
3. Go to the Quick Scan tab in the left part of the window.
4. Click the Run button.

   A progress bar and a button to stop the scan are displayed during the scan. A scan report is displayed when scanning is complete.

Comment

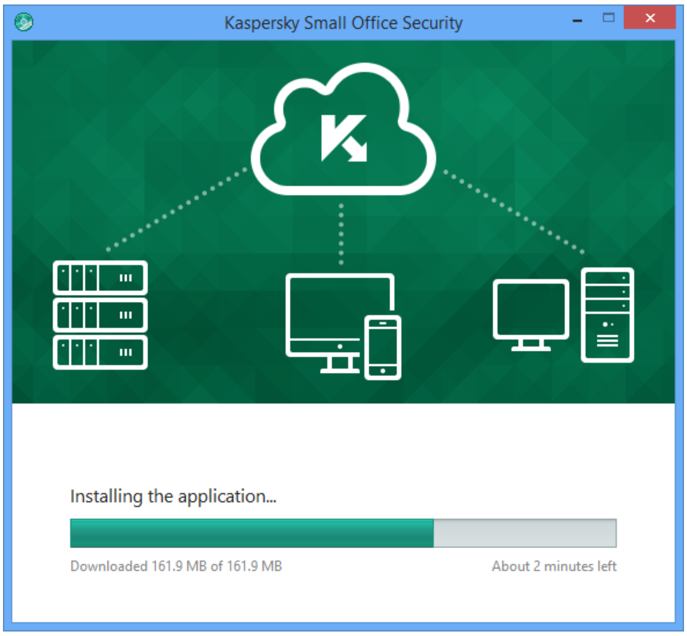
We were struck by the simplicity of the console design, which allows the status of all devices to be seen clearly, and essential tasks such as updates and scans to be carried out, from a single page. We feel that this would enable somebody new to network security management to find their way around easily without any training. We liked the informative tiles for each device, which indicate when scans or updates are running, and clearly show major or minor alerts. We found the console very intuitive and convenient to use, with commands always very visible and easy to access. We were impressed with the speed at which the client software responded to commands from the console. For example, when we started an update on a computer from the console, we could see on the target machine that the process had started to run only a couple of seconds later. We note that the console has been designed with touch interfaces in mind; the Components page pictured above is a good example, with big, finger-friendly sliding buttons for the controls. We particularly liked the very simple, clearly laid-out instructions in the console's help feature, which are obviously very tablet-friendly. We have one suggestion for improvement. To get to the Downloads page to deploy software, the administrator has to click on Licenses and then Usage; we did not find this very intuitive, and suggest that a link could be added to the console in a more prominent position.

Windows client protection software



Installation

Clicking the relevant link in the console/email downloads an exe setup file, which is then run on the target machine. The administrator clicks one button *Install*, then has to decide whether to join the Kaspersky Security Network. After this, the installation proceeds, with a progress display:



Installing the application...

Downloaded 161.9 MB of 161.9 MB

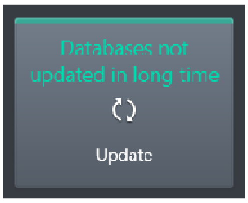
About 2 minutes left

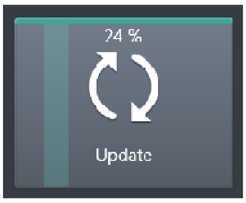
At the end, the administrator just has to click *Finish*, and installation is complete.

Main program window

The main window of KSOS will look familiar to anyone who has used the Kaspersky Internet Security or Anti-Virus consumer products. The essential features status, update and scan all feature their own prominent tiles, and help, support, settings and licence information are all easily accessible from the home page. There are also tiles for the other main features, *Safe Money, Password Manager, Data Encryption,* along with a link to the management console.

When the program is first run, the *Update* tile warns that an update needs to be run; clicking on the tile starts the update, and the tile shows the state of progress:

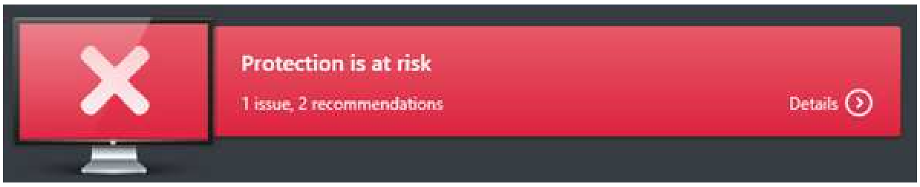




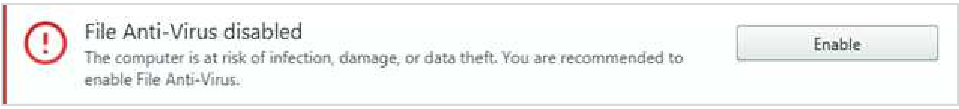
Update tile before update

Update tile during update

If protection is disabled, the status display shows a very prominent warning:



Clicking on the status display bar opens the Notification Center, from which the protection can be re-enabled with a single click:

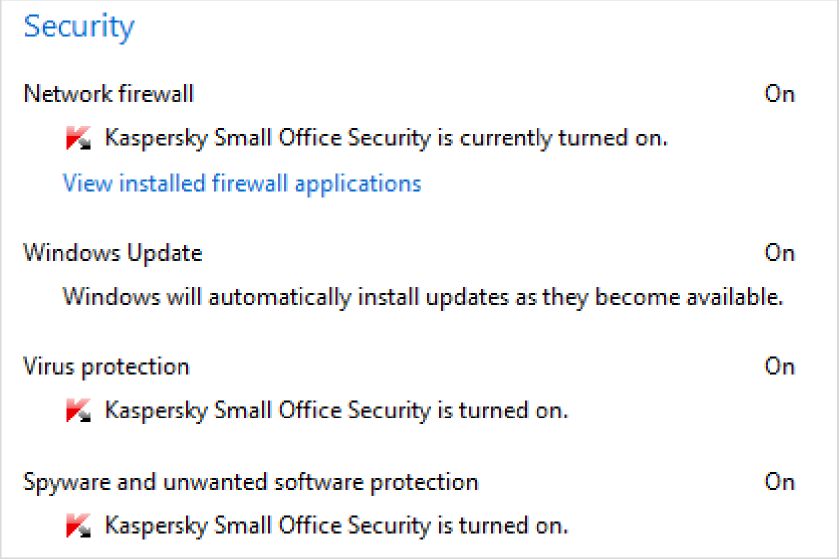


File Anti-Virus disabled

The computer is at risk of infection, damage, or data theft. You are recommended to enable File Anti-Virus.

Windows Action Center

KSOS registers with Windows Action Center as the antivirus, antispyware and firewall:



Security

Network firewall On

Kaspersky Small Office Security is currently turned on.

View installed firewall applications

Windows Update On

Windows will automatically install updates as they become available.

Virus protection On

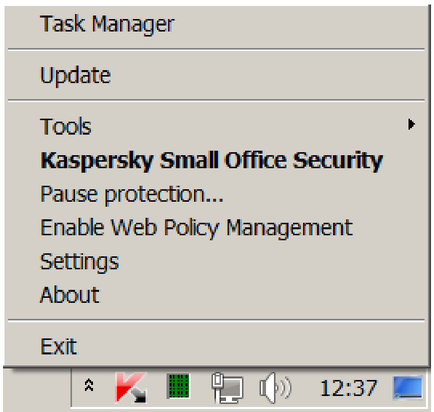
Kaspersky Small Office Security is turned on.

Spyware and unwanted software protection On

Kaspersky Small Office Security is turned on.

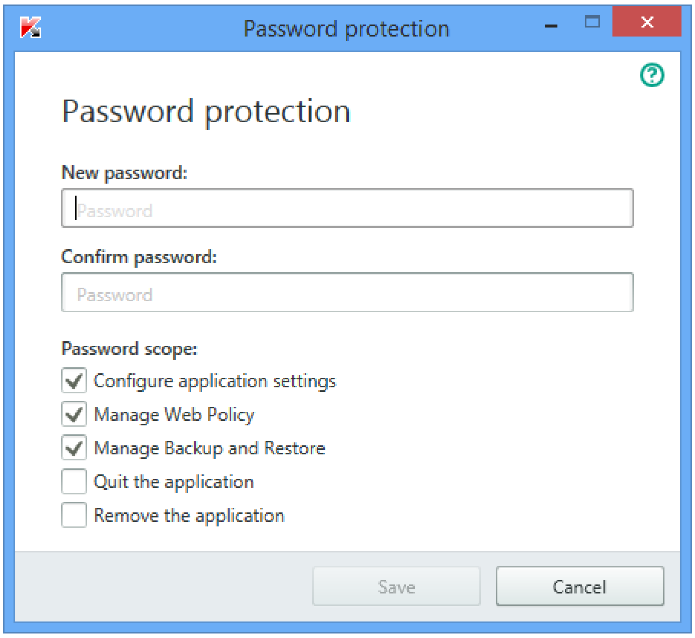
System Tray icon

An icon is displayed in the Windows System Tray. It can be double-clicked to open the main program window, or right-clicked to show a context menu of common tasks:



Unauthorised access

The software can be password protected to prevent unauthorised access. We would strongly recommend administrators to activate this, and to include the options to password protect closing or removing the program:



Password protection

Password protection

New password: Password

Confirm password: Password

Password scope:

☑ Configure application settings

☑ Manage Web Policy

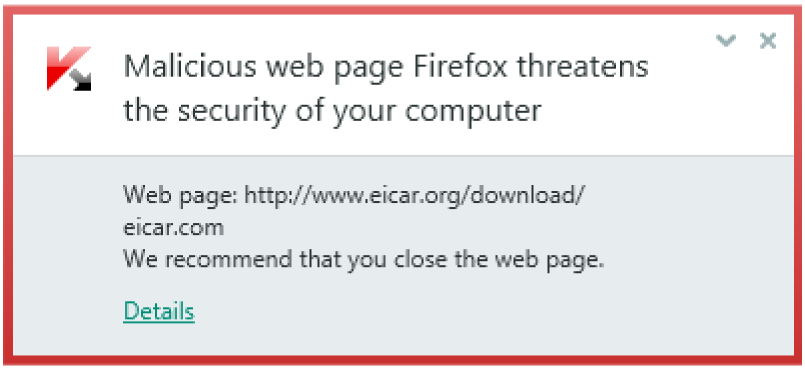
☑ Manage Backup and Restore

□ Quit the application

□ Remove the application

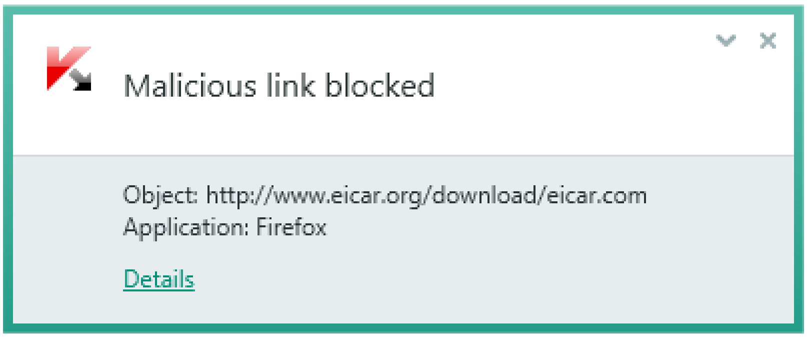
Malware alerts

The following alerts are shown when malware is discovered:



Malicious web page Firefox threatens the security of your computer

Web page: http://www.eicar.org/download/eicar.com
We recommend that you close the web page.



Malicious link blocked

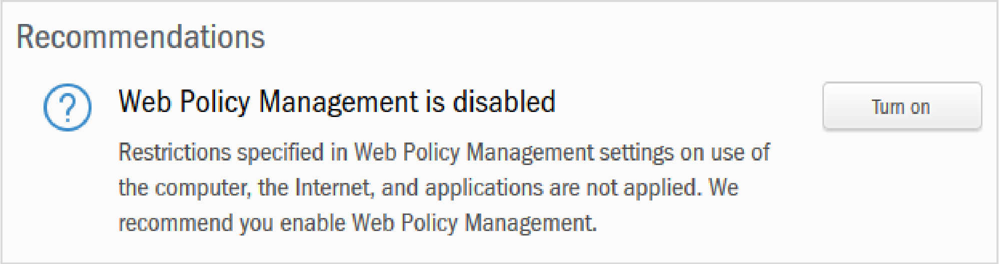
Object: http://www.eicar.org/download/eicar.com
Application: Firefox

Firewall

A Kaspersky Labs firewall is included in the Windows protection software. It is enabled by default on client systems, and takes on the existing public/private network-type setting from Windows. It can be switched off or on from the *Components* section of the management page of each Windows computer.

Web Policy Management

This feature allows the system administrator to place time restrictions on web/Internet access, block specific applications, block sending of confidential information such as credit cards, control who can be contacted on social networks, and prevent particular categories of website from being accessed. The feature can be activated from the for any individual Windows client system by going to its management page:

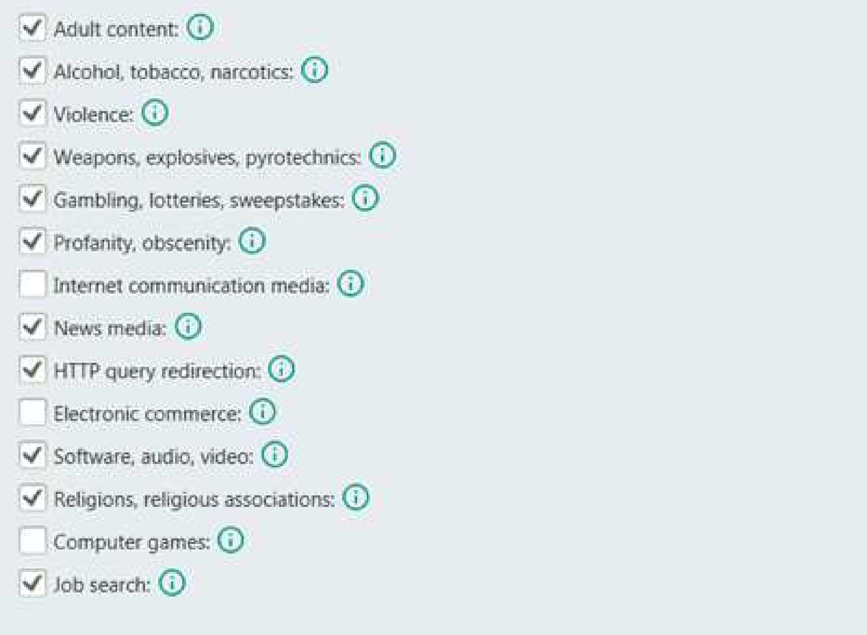


Recommendations

Web Policy Management is disabled

Restrictions specified in Web Policy Management settings on use of the computer, the Internet, and applications are not applied. We recommend you enable Web Policy Management.

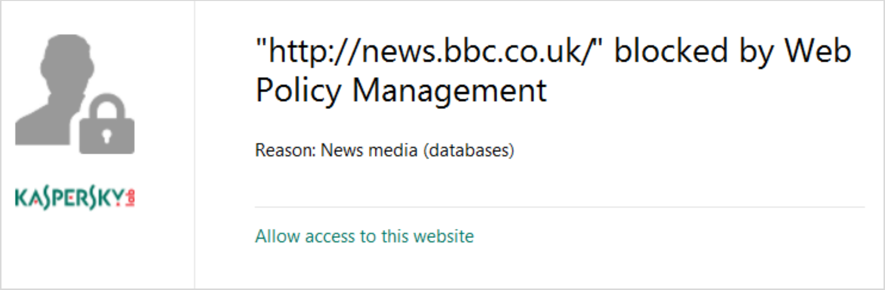
This applies the default setting, which blocks particular categories of website, but does not impose any other restrictions. The categories default blocked are shown below:



☑ Adult content: ⓘ
☑ Alcohol, tobacco, narcotics: ⓘ
☑ Violence: ⓘ
☑ Weapons, explosives, pyrotechnics: ⓘ
☑ Gambling, lotteries, sweepstakes: ⓘ
☑ Profanity, obscenity: ⓘ
□ Internet communication media: ⓘ
☑ News media: ⓘ
☑ HTTP query redirection: ⓘ
□ Electronic commerce: ⓘ
☑ Software, audio, video: ⓘ
☑ Religions, religious associations: ⓘ
□ Computer games: ⓘ
☑ Job search: ⓘ

Please note that the screenshot above is taken from the settings page of a Windows client PC. If the administrator wishes to change the configuration of Web Policy Management, or deactivate it, this has to be done locally on the individual PC. We suspect that many employers would prefer to block computer games and allow news media, and suggest that Kaspersky Lab could change the default category selection accordingly.

When we tested this feature, we found that as soon as it had been activated from the console, websites in these categories were immediately blocked on the client PC, with a Kaspersky block page being shown in the browser:



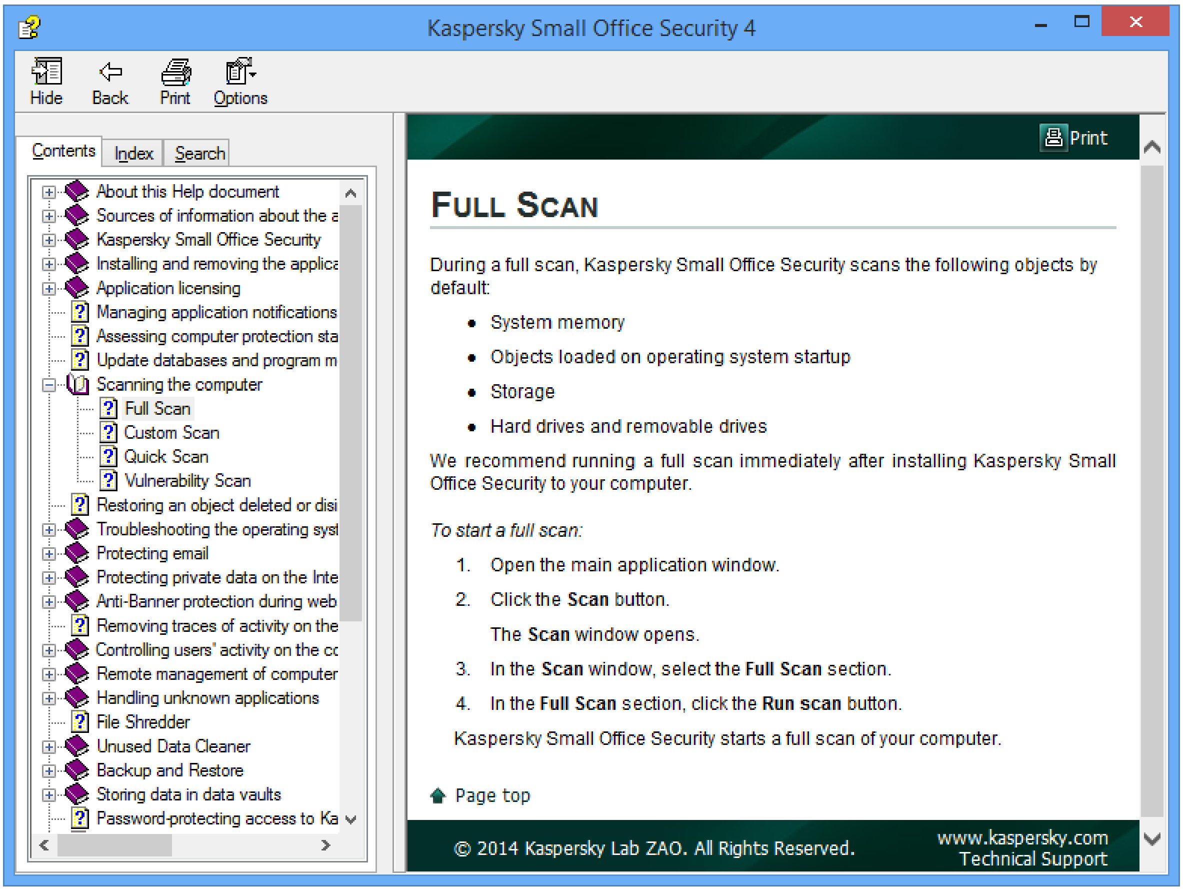
"http://news.bbc.co.uk/" blocked by Web Policy Management

Reason: News media (databases)

Allow access to this website

Integrated help feature

Clicking the *?* symbol in the top right-hand corner of the program window opens a Windows Help window. This provides comprehensive instructions for installing and configuring the software, and using all of its features. The articles relate to managing the software locally rather than via the console, but a section entitled *Remote management of computer* explains how to connect the computer to the management console, thus enabling remote management.


Kaspersky Small Office Security 4
Hide
Back
Print
Options
Contents
Index
Search
About this Help document
Sources of information about the a
Kaspersky Small Office Security
Installing and removing the applica
Application licensing
Managing application notifications
Assessing computer protection sta
Update databases and program m
Scanning the computer
Full Scan
Custom Scan
Quick Scan
Vulnerability Scan
Restoring an object deleted or disi
Troubleshooting the operating syst
Protecting email
Protecting private data on the Inte
Anti-Banner protection during web
Removing traces of activity on the
Controlling users' activity on the cc
Remote management of computer
Handling unknown applications
File Shredder
Unused Data Cleaner
Backup and Restore
Storing data in data vaults
Password-protecting access to Ka
Print

FULL SCAN

During a full scan, Kaspersky Small Office Security scans the following objects by default:

- System memory
- Objects loaded on operating system startup
- Storage
- Hard drives and removable drives

We recommend running a full scan immediately after installing Kaspersky Small Office Security to your computer.

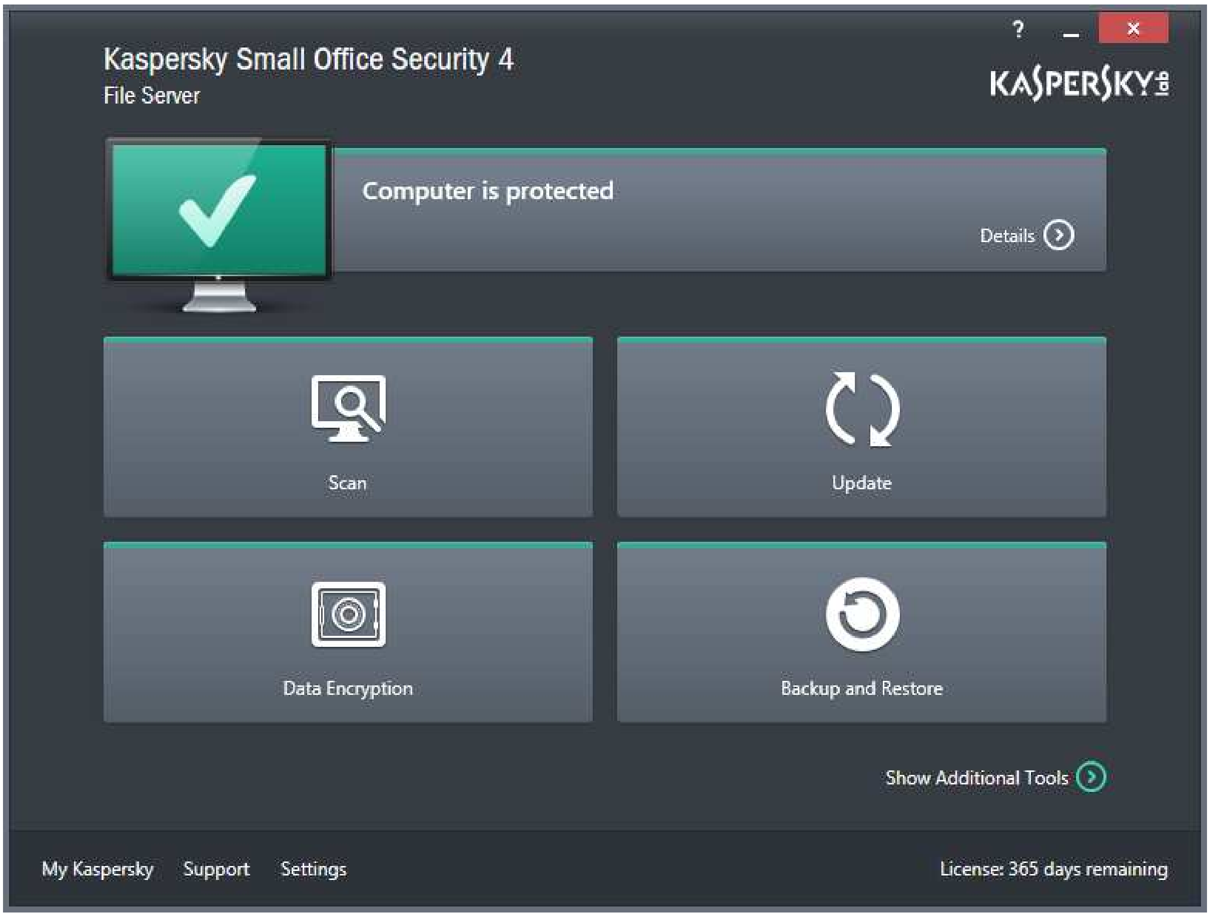
To start a full scan:

1. Open the main application window.
2. Click the **Scan** button.

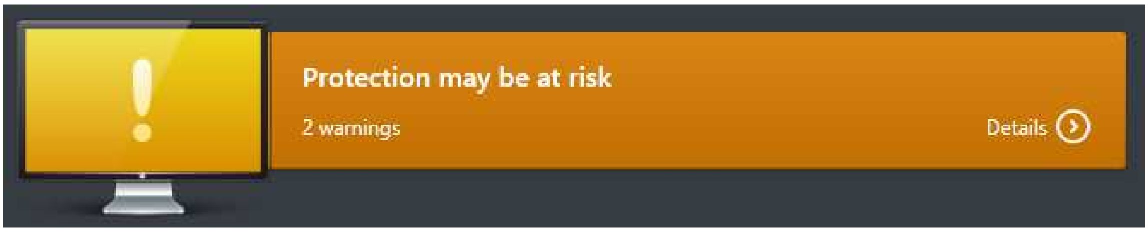
   The **Scan** window opens.
3. In the **Scan** window, select the **Full Scan** section.
4. In the **Full Scan** section, click the **Run scan** button.

Kaspersky Small Office Security starts a full scan of your computer.

Windows server protection software



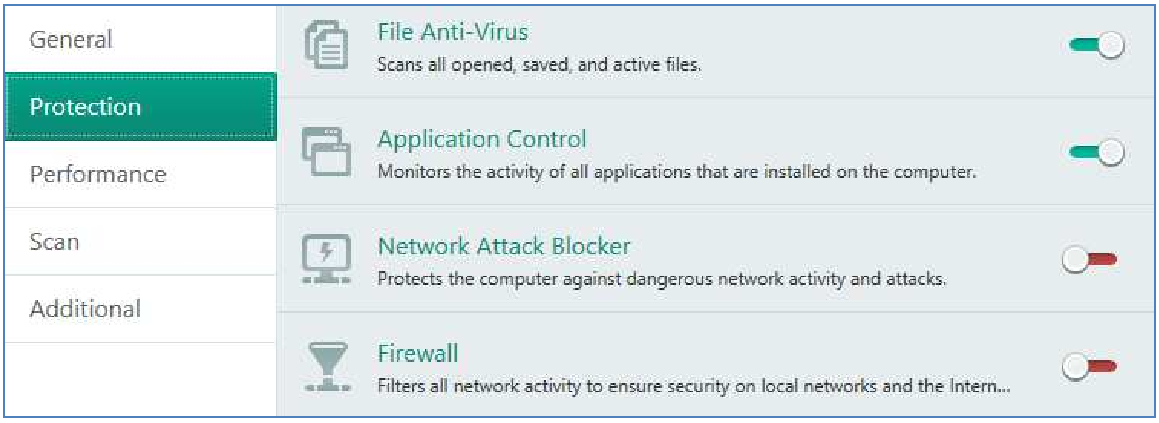
The *File Server* variant of the KSOS windows protection software is very similar to the *Personal Computer* software, except that some features irrelevant to a server (such as *Safe Money* and *Password Manager*) are not included. There are also some configuration differences. For example, the firewall is not activated by default (Windows Server's own firewall is left running), and the option to *Detect other software that can be used by intruders to damage your computer or personal data* is enabled by default. When we downloaded the AMTSO PUA test file, the following warning was shown:



Protection may be at risk

2 warnings

As with its client counterpart, the server protection software is very finger-friendly, making administration from a tablet very easy. As an example, the main *Settings* page is shown below:



File Anti-Virus
Scans all opened, saved, and active files.

Application Control
Monitors the activity of all applications that are installed on the computer.

Network Attack Blocker
Protects the computer against dangerous network activity and attacks.

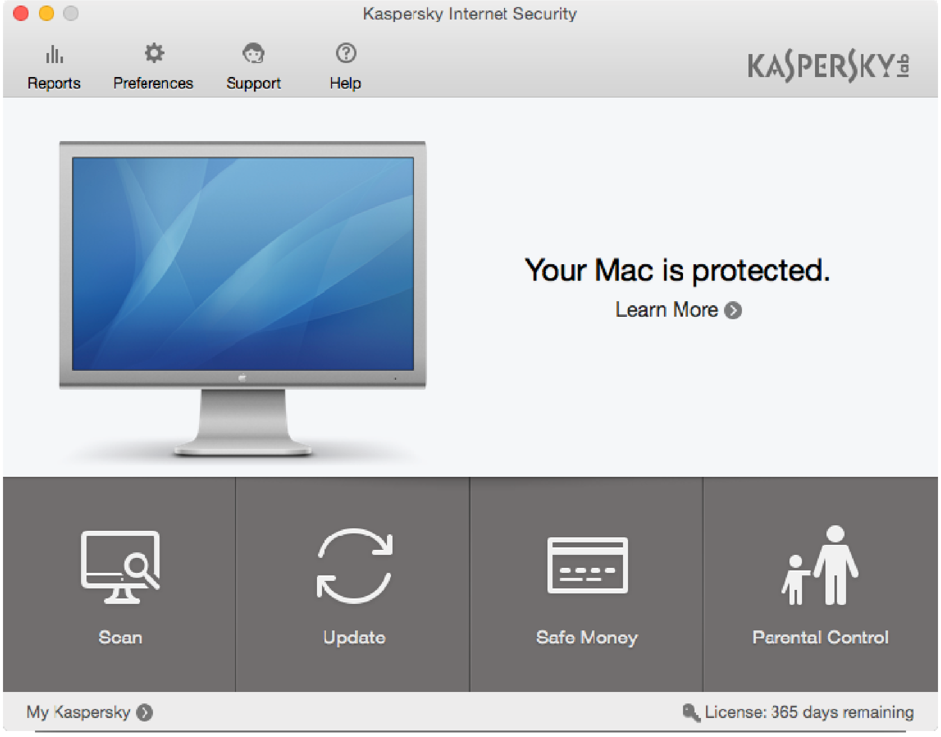
Firewall
Filters all network activity to ensure security on local networks and the Intern...

A complete description of the feature/configuration differences between the client and server versions of the software is provided in the manual.

Comment

We found the Windows protection software, both client and server versions, to be very well designed, with a clear status display and malware warnings, easy rectification of any problems, and all essential information and features easily accessible from the home page. The use of the same interface for both client and server versions simplifies management, and we feel anyone who can use a good consumer antivirus product will easily get to grips with the Windows software in KSOS. We also note the touch-friendly interface design.

Mac client protection software

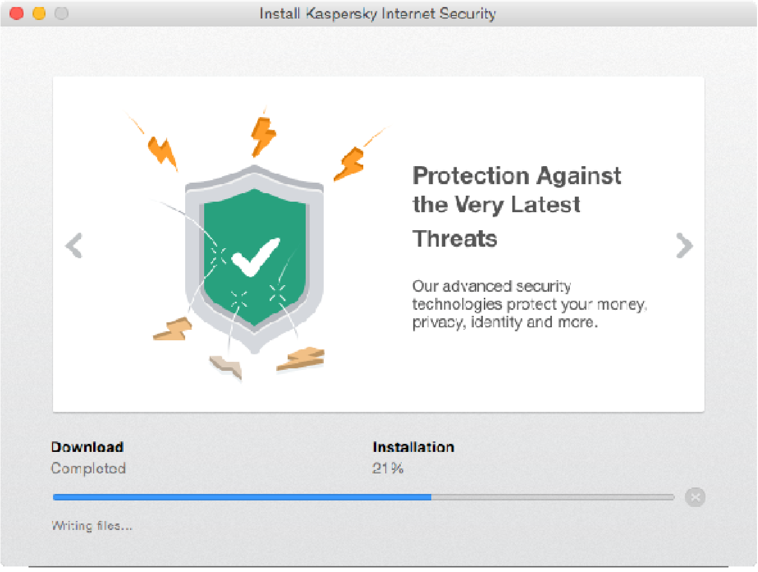


Your Mac is protected.

Learn More

Installation

The .DMG installer file downloaded from the console can be double-clicked to start; the administrator then only has to click *Install…* and decide whether to participate in the Kaspersky Security Network, then click *Download and install*. No further interaction is required, but a progress bar is displayed:



Protection Against the Very Latest Threats

Our advanced security technologies protect your money, privacy, identity and more.

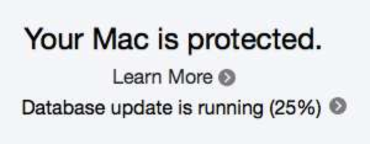
Download
Completed

Installation
21 %

Writing files...

Main program window

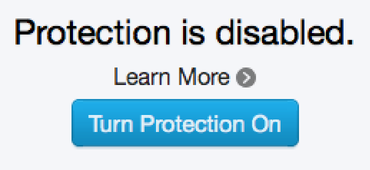
This features a very prominent status display, with the essential functions scan, update, help, settings and licence information all easily accessible from the home page. The status display shows the progress of updates:



Your Mac is protected.

Database update is running (25%) ➜

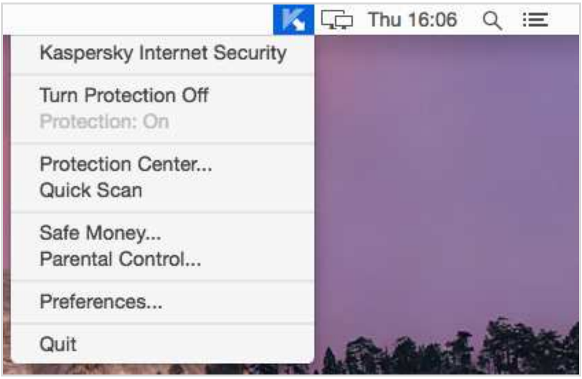
It also shows a warning if protection is disabled, and displays a button with which it can instantly be re-enabled:



Protection is disabled.

System Tray icon

KSOS displays an icon in the OS X System Tray, which shows a menu of common tasks:

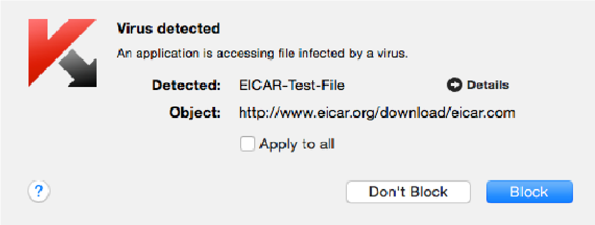


Unauthorised access

The protection features can only be configured by entering administrator credentials for Mac OS X, preventing standard users from disabling them.

Malware alerts

The following alert is shown when malware is discovered:



Virus detected

An application is accessing file infected by a virus.

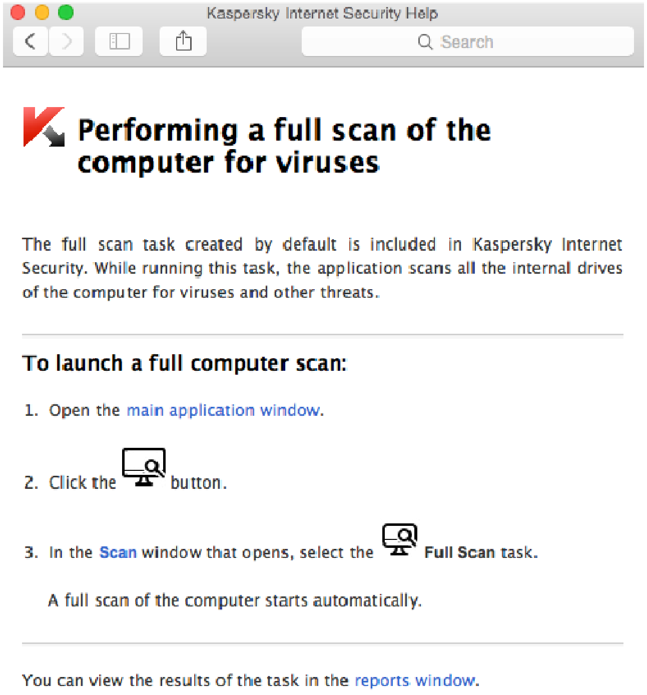
Detected: EICAR-Test-File

Object: http://www.eicar.org/download/eicar.com

□ Apply to all

Integrated help feature

Clicking the *Help* button on the menu bar at the top of the program window opens the local help service, which provides simple text instructions for all the features of the product. There are no screenshots as such, but as illustrated below, icons are shown when applicable:



Performing a full scan of the computer for viruses

The full scan task created by default is included in Kaspersky Internet Security. While running this task, the application scans all the internal drives of the computer for viruses and other threats.

To launch a full computer scan:

1. Open the main application window.
2. Click the button.
3. In the Scan window that opens, select the **Full Scan** task.

   A full scan of the computer starts automatically.

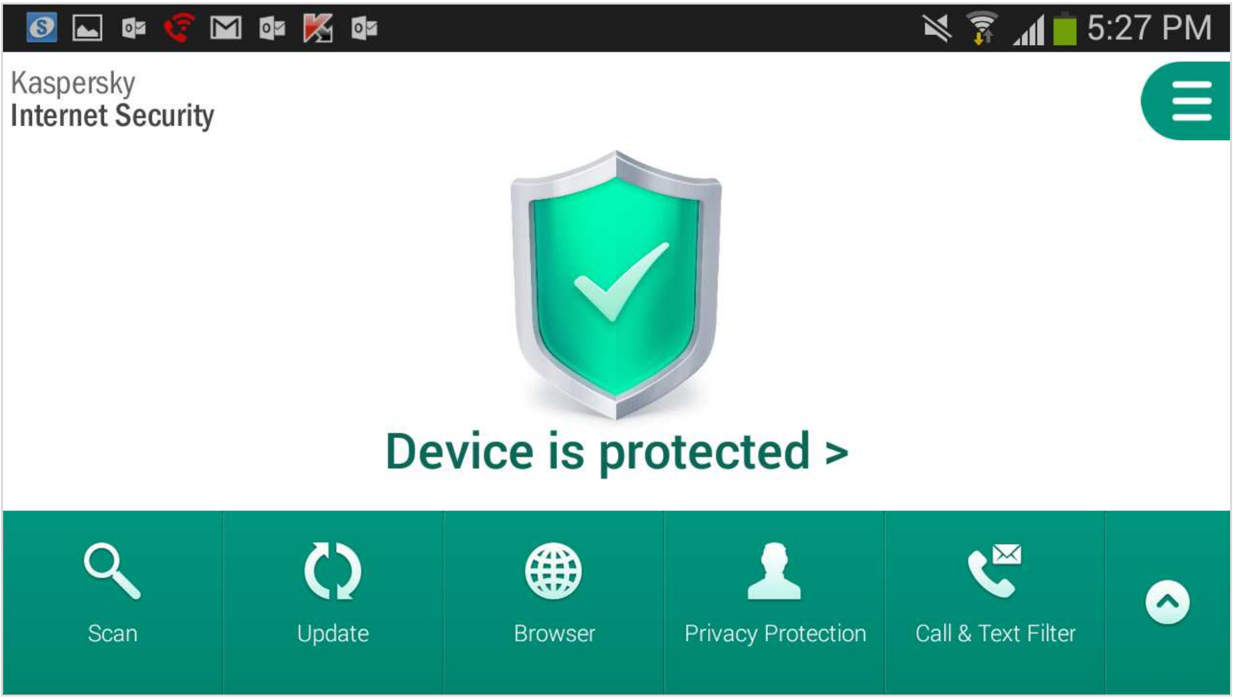
You can view the results of the task in the reports window.

The *My Kaspersky* portal is mentioned in one of the articles, which states that it can be used to "manage protection of computers with Kaspersky Total Security [sic] installed". Kaspersky Total Security is Kaspersky Lab's multi-device consumer product. The article does not state how to connect an unmanaged device to the console.

Comment

We feel the Mac client software will prove very easy to use for anyone, especially if they are accustomed to Windows antivirus software. There is a clear status display, which warns in the event of a problem and makes this easy to rectify. All the essential functions are easy to find in the program's home page.

Android client software


5:27 PM

Kaspersky
Internet Security

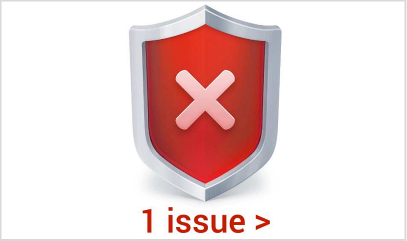
Device is protected >

Installation

Kaspersky Internet Security for Android is installed via Google Play (setup can be started clicking the installation link in the console). Once the program has been installed, the theft protection feature can be activated; this can be done tapping on its icon in the main screen. The process involves making KISA a device administrator, but is short and simple.

Main program window

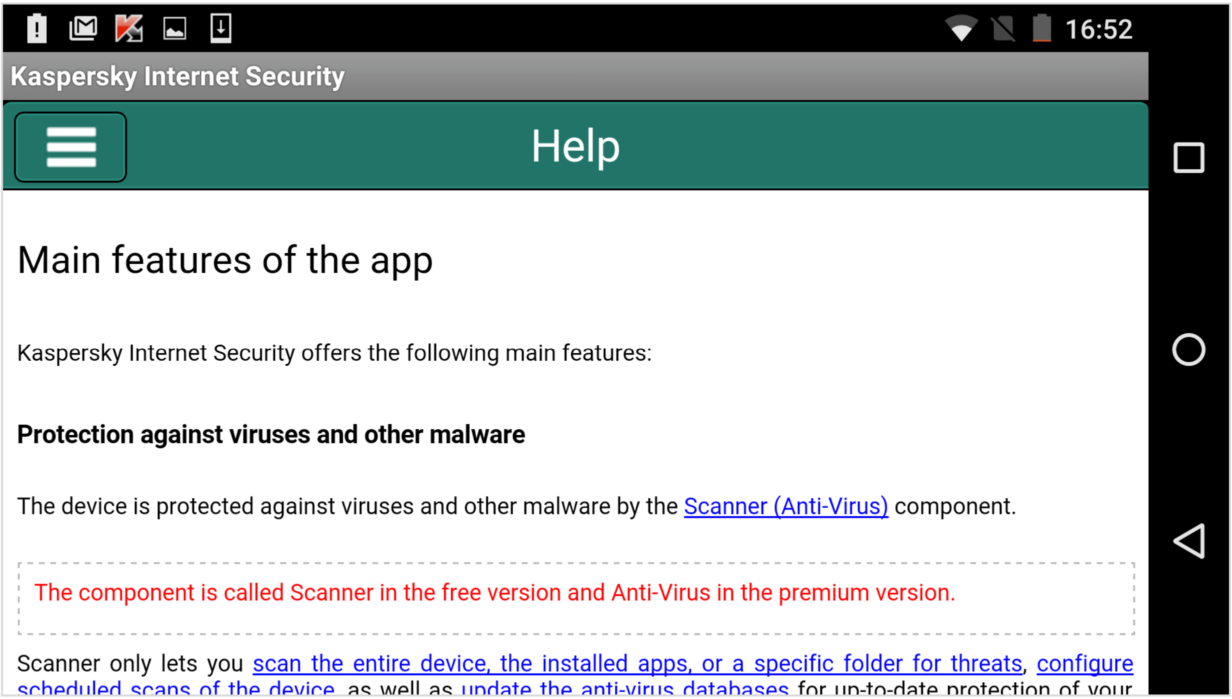
Status, scan and update functions are displayed directly on the main screen. Settings and help, along with icons for features such as theft protection, can be found by tapping the up-arrow symbol in the bottom right-hand corner of the screen. If protection is disabled, the status display shows a clear warning:


1 issue >

Tapping *1 issue* opens the configuration page from which protection can be re-enabled.

Integrated help feature

Tapping the *Help* button on the app's home screen opens the integrated help, which has text articles covering all the product's features:



Main features of the app

Kaspersky Internet Security offers the following main features:

Protection against viruses and other malware

The device is protected against viruses and other malware by the Scanner (Anti-Virus) component.

The component is called Scanner in the free version and Anti-Virus in the premium version.

Scanner only lets you scan the entire device, the installed apps, or a specific folder for threats, configure scheduled scans of the device, as well as update the anti-virus databases for up-to-date protection of your

We could not find any reference to connecting the product to the KSOS Management Console.

Comment

We found the Android client software very easy to use. We particularly liked the arrow at the end of the menu bar, which toggles between showing all features or just the most important ones.

Summary

Version 4 of Kaspersky Small Office Security features a new cloud-based console for management of Windows clients and servers, Mac OS clients, and Android mobile devices. This means that laptops and mobile devices can be managed even when not connected to the office network, and the administrator can use any Internet-connected computer, tablet or smartphone to manage devices.
The console does not require any sort of installation or configuration; once a Kaspersky account has been created, the console is ready to use. Deploying the protection software from the console is very easy. The administrator clicks on the appropriate link on the Downloads page to start the process. For Windows and Mac software, the installer can be saved and run locally, or saved to a flash drive for local deployment on other machines. It is also very easy to email a link to remote users, with which they can download and install the software themselves. The console is very simple and clear, and consequently makes it very easy to see the status of protected devices and carry out essential tasks. Whilst all administrators will appreciate the very clean and uncluttered design, we feel it is especially well suited to novice administrators encountering a security management console for the first time. Whilst the console does not provide as much functionality as products designed for bigger businesses, we feel that the clarity and ease of use more than compensate for this. We particularly liked the status tiles for each device, which show very clearly whether the device is online, what its security status is, and if scans or updates are running. If a problem is shown on a device, it can be very easily rectified by clicking its *Manage* button.

We were impressed with the speed at which devices respond to console commands, with just a couple of seconds elapsing between e.g. sending a *Scan* command from the console, and the task starting on the device. Both the management console and the Windows protection software have been designed with touch screens in mind, and both can be used very easily on a tablet. All the individual protection programs (for Windows, Mac OS and Android) are very well-designed and user-friendly, and will prove instantly familiar to anyone who has used a similar consumer security product. Each has its own detailed manuals and knowledge-base articles, as well as local help services. The console's help page is very clearly and simply laid out, making it very easy to find a particular article.

Kaspersky Lab have informed us that they are reviewing the documentation for the product. We have a couple more suggestions for improvement:

1. The difference between my.kaspersky.com and center.kaspersky.com should be explained
2. The console should have an easy-to-find link to the *Downloads* page
3. The default Web Policy Management settings should be more business-oriented

In summary, Kaspersky Small Office Security 4 is extremely well suited to a small-business network without professional IT support. Deploying and managing the protection software from the console should be a straightforward task for anyone who can install and use iTunes. The product is a very obvious choice for small companies who want centrally managed, professional security software for a server, Windows and Mac desktops and laptops, and Android mobile devices, without having to employ dedicated IT staff to look after it.

Copyright and Disclaimer

AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

(June 2015)