Anti-Virus Comparative

Summary Report 2012

Awards, winners, comments

Language: English
December 2012
Last Revision: 5th January 2013

www.av-comparatives.org

Table of Contents

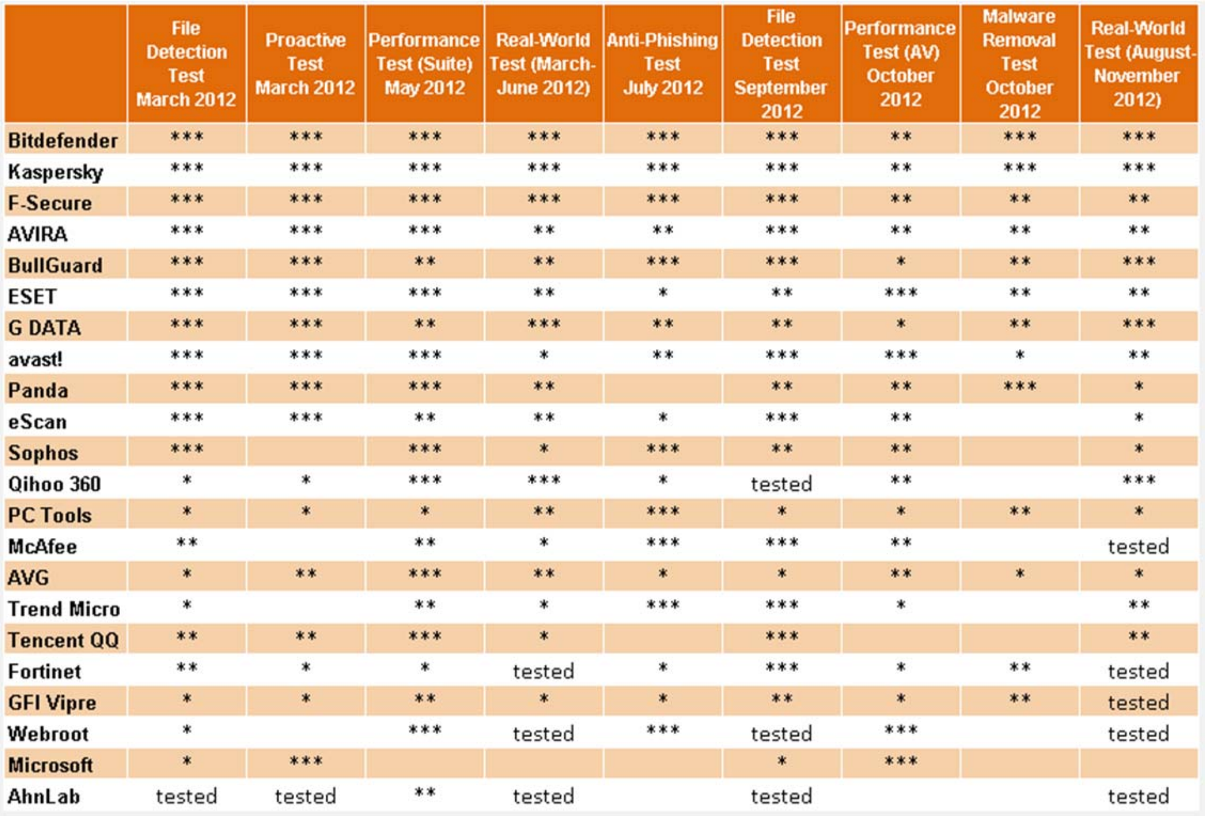
Introduction

At the end of every year, AV-Comparatives releases a summary report to comment on the various anti-virus products tested over the year, and to mention again the high-scoring products of the various tests. Please bear in mind that this report looks at all the comparative tests of 2012, i.e. not only the latest ones. Comments and conclusions are based on the results shown in the various comparative test reports of AV-Comparatives, as well as from observations made during the tests (http://www.av-comparatives.org/comparativesreviews). Products which are available only in Chinese language are only listed in the Chinese version of this report (available on our website).

Overview of levels reached during 2012

It is important that readers understand that the STANDARD level/award is already a good score, since it requires a program to reach a certain standard of quality. Additionally, all the products tested are security programs from reputable and reliable manufacturers.

Below is an overview of levels/awards reached by the various anti-virus products in AV-Comparatives' tests of 2012. Vendors, who did not want to see some features of the product evaluated, renounced being considered for the summary awards.



	File Detection Test March 2012	Proactive Test March 2012	Performance Test (Suite) May 2012	Real-World Test (March-June 2012)	Anti-Phishing Test July 2012	File Detection Test September 2012	Performance Test (AV) October 2012	Malware Removal Test October 2012	Real-World Test (August-November 2012)
Bitdefender	***	***	***	***	***	***	**	***	***
Kaspersky	***	***	***	***	***	***	**	***	***
F-Secure	***	***	***	***	***	***	**	**	**
AVIRA	***	***	***	**	**	***	**	**	**
BullGuard	***	***	**	**	***	***	*	**	***
ESET	***	***	***	**	*	**	***	**	**
G DATA	***	***	**	***	**	**	*	**	***
avast!	***	***	***	*	**	***	***	*	**
Panda	***	***	***	**		**	**	***	*
eScan	***	***	**	**	*	***	**		*
Sophos	***		***	*	***	**	**		*
Qihoo 360	*	*	***	***	*	tested	**		***
PC Tools	*	*	*	**	***	*	*	**	*
McAfee	**		**	*	***	***	**		tested
AVG	*	**	***	**	*	*	**	*	*
Trend Micro	*		**	*	***	***	*		**
Tencent QQ	**	**	***	*		***			**
Fortinet	**	*	*	tested	*	***	*	**	tested
GFI Vipre	*	*	**	*	*	**	*	**	tested
Webroot	*		***	tested	***	tested	***		tested
Microsoft	*	***				*	***		
AhnLab	tested	tested	**	tested		tested			tested

Although STANDARD is already a good score, tests in which a STANDARD award (or lower) was reached indicates areas which need further improvement compared to other products. ADVANCED indicates areas which may need some improvement, but are already very competent.

Winners

If you plan to buy an anti-virus program, please visit the vendor’s website and evaluate their software by downloading a trial version, as there are also many features and important considerations (e.g. compatibility, graphical user interface, ease of use, price, support etc.) that you should evaluate for yourself. As explained above, the perfect anti-virus program or the best one for all needs and for every user does not exist. Our winners’ category is based on test results and does not evaluate or consider other factors that may be of importance for specific users’ needs or preferences. Being recognized as “Product of the Year” does not mean that a program is the “best” in all cases and for everyone; it only means that its overall performance in our tests throughout the year was consistent and unbeaten. The Product of the Year award depends on the number of Advanced+ awards received in all our tests. As all products receiving an Advanced+ award are considered (statistically speaking) to be as good as each other, a product can receive the Product of the Year award without necessarily reaching the highest score in any individual test.

Overall winner of 2012 (Product of the Year)

For AV-Comparatives’ “Product of the Year“ award, all tests in the public main-test series are taken into consideration.

As we give only one Product of the Year Award, we apply the following rule: if there are two or more products with equal marks, the award goes to the product which has not previously received it. The other high-scoring product(s) will be given the Top Rated Award. This means that in the event of two products achieving the same results, the product that has not already won the award will receive it. This year we have precisely this situation: both **Kaspersky** Lab’s and **Bitdefender**’s products were equally good, and both worthy of the Product of the Year award. Bitdefender has not won the award before (and also achieved slightly higher scores in the Real-World Protection Test). Consequently, the 2012 Product of the Year award goes to:

Bitdefender

Top Rated Products 2012

This year, like last year, a number of products reached a very high standard in all our tests. Although we still only have one Product of the Year, we have decided to recognise all those products with good overall results by giving them the AV-Comparatives Top Rated award.

This year, like last year, a number of products reached a very high standard in all our tests. Although we only have one Product of the Year, we recognise all those products with good overall results by giving them the AV-Comparatives Top Rated award.

We have used the results over the year to designate products as “Top Rated”. Results from all the tests are assigned points as follows: Tested = 0, Standard = 5, Advanced = 10, Advanced+ = 15. Products with 105 points or more were given the Top Rated award, with two conditions. Firstly, any products that failed to win any award (i.e. got 0 points) in the Real World Protection tests have not been considered. Secondly, good results in the performance tests cannot make up for weak results in the detection/protection tests.

Top Rated products for 2012 are

Avast - AVIRA - Bitdefender - BullGuard

ESET - F-Secure - G DATA - Kaspersky

Please see our awards and summary pages – links below:

http://chart.av-comparatives.org/awardslist.php?year=2012

Whole-Product "Real-World" Dynamic Protection winners

Security products include various different features to protect systems against malware. Such protection features can be taken into account in the Whole-Product Dynamic Protection tests, which test products under real-world conditions. Products must provide a high level of protection without producing too many false alarms, and without requiring the user to make many decisions. The figure shown is the average result over the year: ***Bitdefender*** (99.7%, few FPs), ***G DATA*** (99.6%, few FPs) and ***Kaspersky*** (99.3%, few FPs) all received the Advanced+ award in both tests of 2012.

AWARDS

AV
comparatives
DYNAMIC
PROTECTION
2012
GOLD

Bitdefender

AV
comparatives
DYNAMIC
PROTECTION
2012
SILVER

G DATA

AV
comparatives
DYNAMIC
PROTECTION
2012
BRONZE

Kaspersky

For details and full results of the 2012 Real-World Protection tests, please click the link below:

http://www.av-comparatives.org/comparativesreviews/dynamic-tests

File Detection winners

The File Detection Test evaluates the static file scanning engine component, which is one subset of the protection features provided by security products. A high detection rate of malware - without causing too many false alarms – is, depending on the situation, still one of the most important, deterministic and reliable features of an anti-virus product (as e.g. it is not heavily dependent on infection vectors and other factors).

The following products received the ADVANCED+ award in both overall File Detection tests, in March and September 2012. The figure shown is the average of the two test results: ***AVIRA*** (99.6%), ***Kaspersky*** (99.3%) and ***Bitdefender, F-Secure*** (98.9%).

AWARDS

AVIRA

Kaspersky

Bitdefender, F-Secure

For details and full results of the 2012 File Detection tests, please click the link below:

http://www.av-comparatives.org/comparativesreviews/detection-test

Proactive (Heuristic/Behavioral) Detection/Protection winners

The Proactive test shows how good the heuristic detection and behavioural protection features of the various anti-virus products are (how good they are at detecting new/unknown malware) without Internet access against completely new (0-day) malware. A high proactive detection/protection rate must be achieved with a low rate of false alarms.

The following products showed the highest proactive protection rates in the 2012test: ***Bitdefender***, ***Kaspersky*** (97%, few FPs), ***F-Secure*** (91%, few FPs) and ***G DATA*** (90%, few FPs).

AWARDS

Bitdefender, Kaspersky

F-Secure

G DATA

For details and full results of the 2012 File Detection test, please click the link below:

http://www.av-comparatives.org/comparativesreviews/retrospective-test

False Positives winners

False positives can cause as much trouble as a real infection. Due to this, it is important that anti-virus products undergo stringent quality assurance testing before release to the public, in order to avoid false positives. The products with the lowest rate of false positives during 2012 were ***Microsoft*** (0), ***ESET*** (6), ***Bitdefender*** and ***Kaspersky*** (14). These figures represent the SUM of the false positives from both FP Tests.

AWARDS

Microsoft

ESET

Bitdefender, Kaspersky

For details and full results of the 2012 False Positive tests, please click the link below:

http://www.av-comparatives.org/comparativesreviews/false-alarm-tests

Overall Performance (Low-System-Impact) winners

Anti-virus products must remain turned on under all circumstances, while users are performing their usual computing tasks. Some products may have a higher impact than others on system performance while performing some tasks. ***Webroot***, ***ESET*** and ***Avast*** demonstrated a lower impact on system performance than others.

AWARDS

Webroot

ESET

Avast

For details and full results of the 2012 Performance tests, please click the link below:

http://www.av-comparatives.org/comparativesreviews/performance-tests

Anti-Phishing Protection winners

Phishing websites attempt to steal money from their victims without making any changes to the computer or device being used to access them. A security product that warns of known/suspected phishing sites can protect the user from fraud. The products with the highest blocking rate of phishing websites were ***Bitdefender*** (97.4%), ***McAfee*** (97.0%) and ***Kaspersky*** (94.8%).

AWARDS

Bitdefender

McAfee

Kaspersky

For details and full results of the 2012 Anti-Phishing test, please click the link below:

http://www.av-comparatives.org/comparativesreviews/anti-phishing-test

Malware Removal winners

A very useful ability for an anti-virus program is removal of malware which has already infected a system. In this year's test, ***Bitdefender***, ***Kaspersky*** and ***Panda*** received the Advanced+ award.

AWARDS

AV
comparatives
MALWARE
REMOVAL
2012
GOLD

Bitdefender, Kaspersky

AV
comparatives
MALWARE
REMOVAL
2012
SILVER

Panda

For details and full results of the 2012 Malware Removal test, please click the link below:

http://www.av-comparatives.org/comparativesreviews/removal-tests

User-Interface Review Section

Important note

The awards and certifications mentioned in this report are based purely on our test results. The program reviews in this section are based on our own observations and opinions; whilst we feel these may be helpful to readers, they do not have any effect on the awards. We strongly recommend potential buyers of any of the programs in this report to evaluate the software themselves by using a trial version, and to consider other factors which we have not looked at here (such as compatibility, price and technical support), before deciding to use a particular product.

As in previous years, we have described the graphical user interface of the programs reviewed, along with their use in everyday situations. Please note that for the sake of convenience, we have in places used the term "suite" to refer to all the programs, although in a few cases this is not strictly true. We feel that this small technical inaccuracy results in a more readable report.

Components

We list the major protection components included in the suite, such as antimalware, antispam, firewall, parental control, backup, and shredder. In the case of simple antivirus programs, we also note whether an email scanner is included. We have not listed safe search as a separate feature as we consider it to be part of the antimalware component (it is relevant to the results of the Real-World Protection Test.

Installation

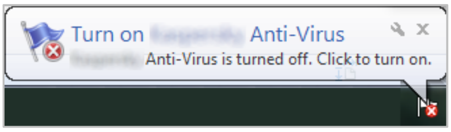
In this section, we have looked at the installation process to see if it is simple for non-expert users, and options are provided for advanced users. If a custom installation option is available, we choose this, but accept the defaults, with one exception: we do not install any third-party software offered by the installer. We consider whether the installation file is a full installation package, a small downloader file, or if both are available. Some setup files contain a complete package, but download any updates available, which we consider to be optimal.

We check whether it is possible to choose the components of the Internet security suite, so that advanced users could use Windows Firewall or an alternative antispam program if they chose to, and if multiple user interface languages are available.

We report when the suite asks about the network type, i.e. whether it is to be regarded as public or private, and thus whether file and printer sharing etc. should be allowed.

We check to see whether the program registers itself in Windows Action Center as an antivirus program, antispyware program, and firewall, and whether it disables Windows Defender and/or Windows Firewall. We would normally expect a suite with its own firewall to disable Windows Firewall to prevent conflicts. We also check to see what Windows Action Center reports if the suite's real-time protection or firewall is disabled.

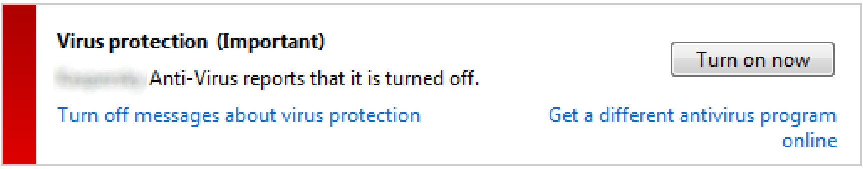
When an important security component is switched off, we would expect Windows Action Center to show a red symbol with a cross in the System Tray icon, and display a warning message, as shown below:



Turn on [redacted] Anti-Virus

[redacted] Anti-Virus is turned off. Click to turn on.

We would also expect a red warning message in the Action Center window, like this:



Virus protection (Important)

[redacted] Anti-Virus reports that it is turned off.

Turn on now
Turn off messages about virus protection
Get a different antivirus program online

We regard Action Center/Security Center as an important tool in assessing the security state of a computer, and that any security program should register its components on installation, and trigger Windows' normal alerts if any of them are not working.

Finally we look at each suite's uninstall programs, to see if there are any options such a repair, or adding/removing individual components.

Program interface

In describing each program's main window, we have concentrated on what we feel are the most important elements: a status display, showing whether important protection components such as real-time antivirus are up-to-date and working correctly; a warning if they are not, and an easy means of correcting this, such as a Fix-All button; an Update button, to download the latest malware definitions (not applicable in some cloud-based programs); a Scan button, enabling full and custom scans to be run; a Help button; and subscription information (obviously not applicable with free programs). We also check to see if the suite has added entries to Windows Explorer's context menu, so that files and folders can be scanned simply by right-clicking them.

Default configuration

In this section of the review, we have looked at the default configuration for each suite regarding firewall settings, and the messages displayed/action taken when malware is discovered. We have especially considered the needs of non-expert users, who largely require the software to make sensible decisions for them, rather than ask questions they cannot understand.

Non-administrator access

We check whether standard (non-administrator) Windows accounts are able to deactivate important components such as real-time protection or the firewall. We feel this is important for family computers, where younger children have been assigned standard user accounts to prevent them from making system changes.

Scanning and malware discovery

We have looked at how to configure a scheduled scan, and whether one is set by default. We also consider whether it is possible to do a boot-time scan, to remove malware before the Windows interface has loaded.

We next check how each suite reacts when malware is discovered, using a variety of situations. We must stress that this is NOT a detection test; the aim is to see what action the suite takes when malware is detected, and how it informs the user. We feel that to be suitable for non-expert users, a suite should either take action automatically or present a very clear default option (quarantine being ideal in both cases). Where it takes action automatically, the program should make clear that it has done so, and that no further action needs to be taken.

Before carrying out the tests, we disable Microsoft's Windows Defender and SmartScreen Filter to prevent interference. In the first test, we attempt to download the EICAR test file from www.eicar.org and note the result. For the remaining tests, we copy a few common Trojans packed in a password-protected zip file to our test PC, and then deliberately disable the real-time protection in order to unpack the malware files into a normal folder. We then reactivate real-time protection, and open the malware folder. In some cases, the real-time protection is so sensitive that it will detect the malware at this point. If not, we right-click a file and select Properties, causing Windows to read the file's contents, and so trigger detection.

For the next test, we disable real-time protection once more, unpack the malware again, and then run a context-menu scan of the folder (with the exception of a couple of programs which do not provide this facility). Finally we repeat this procedure but run a custom scan on the folder from the program interface.

Inbound firewall settings

When creating the Windows image to be used on our test PC, we set the network type to Work, and enabled file and printer sharing in Windows Network and Sharing Center; we also set up a file share with a text document in, which could then be opened and edited from another computer on the same network.

During the setup process for each suite, if we are asked whether the PC's current network should be regarded as public or private, we always select private, meaning that file sharing should continue to function after the suite has been installed. When each suite is up and running, we test firstly whether we can ping the test PC from another computer on the LAN, and then whether it is possible to open, edit and save the text file in the file share.

We then disable the existing network connection (Ethernet) on our test PC, and connect to a wireless network with a completely different subnet. When prompted by Windows Network and Sharing Center as to the network type, we select Public, to simulate connecting to a wireless network in a café or hotel. If the suite's own firewall displays its own query about the network type, we select the most appropriate option for a public network. We then try to ping the test PC, access its file share, and log on with Remote Desktop (using both hostname and IP v4 address), from another computer on the new "public" network. We would expect all access to be blocked if the firewall is working properly; this would be the result with Windows Firewall. In the case of the programs that did not contain their own firewall, but used Windows Firewall, this section was redundant.

Outbound firewall/application control

In order to test the outgoing firewall/application control settings of each suite, we developed a simple program which we describe as a firewall tester. This simply attempts to contact an FTP server over the Internet, and download a text file. This assesses whether the default settings of the suite block the program's operation, allow it without question, or query whether it should be allowed. We must again stress that this is NOT a detection test; the program is entirely harmless and should not be recognised as malicious. In fact, we would argue that if it is to be regarded as suitable for beginners, a suite should allow the firewall tester to complete its task without any form of restriction and without asking any questions. We are of the opinion that asking non-expert users whether to allow a particular program or process to access the Internet is totally counter-productive; the user will almost certainly not be able to make an informed decision, and will probably either allow all requests or block all requests, making the process either pointless or even actually destructive.

In the event that the firewall tester completed its task without query, we looked for firewall/application control settings which would ask if the program should be allowed; we consider this to be a valid option for advanced users. If the suite's default action is to ask about allowing the firewall tester, we checked to see if there is a setting which will switch this behaviour off.

We ran this test with all the programs we reviewed; however, in the case of programs that only used Windows Firewall we did not feel it was necessary to mention the result in the report. When the firewall tester is run on a system using only Windows Firewall with default configuration, there is no interaction or interference from the firewall at all, and the test completes successfully without any interference or query.

Safe Mode

In order to remove a malware infection from a PC, it can be valuable to start in Safe Mode. To test how each security program would function in Safe Mode, we copied our zip file of malware programs to the test PC, and then started in Safe Mode with Networking. We unzipped the malware files into a folder on the desktop. Next, we attempted to open the security suite's program window; enable real-time protection; run an update (hence Safe Mode with Networking); run a custom scan on the malware folder. We also attempted to run a scan on the malware from Windows Explorer's context menu – this was the only option available in cases where we could not open the program window. We must stress that this is NOT a malware removal test; all the samples were inactive. We were only testing each program's ability to function in Safe Mode on an entirely clean and functional PC.

Help and documentation

The final area we considered for each security program was the help functions. We looked for both local help (i.e. help files installed on the local PC) and online help, i.e. pages of the manufacturer's website, and downloadable manuals. Conducting a full review of the entire help and documentation available for 22 programs would be a mammoth task, so to get a rough idea of the usefulness of the help functions, we searched for answers to two questions in both local and online help (where both existed). We attempted to find out how to set a scheduled scan, and how to exclude a folder from scans. We felt that these were questions many users might want answered, and so a reasonable help function should cover them. We tried slightly different search terms depending on whether we expected complete sentences to be understood ("How do I… ?") and whether previous searches had been successful. For example, if "scan exceptions" had not produced any relevant results, we tried "scan exclusions".

We consider a useable help function to be important in a security program, especially for non-expert users. It can also be very helpful to advanced users if the interface is complicated and particular features or settings are hard to find.

Scanning without cloud access

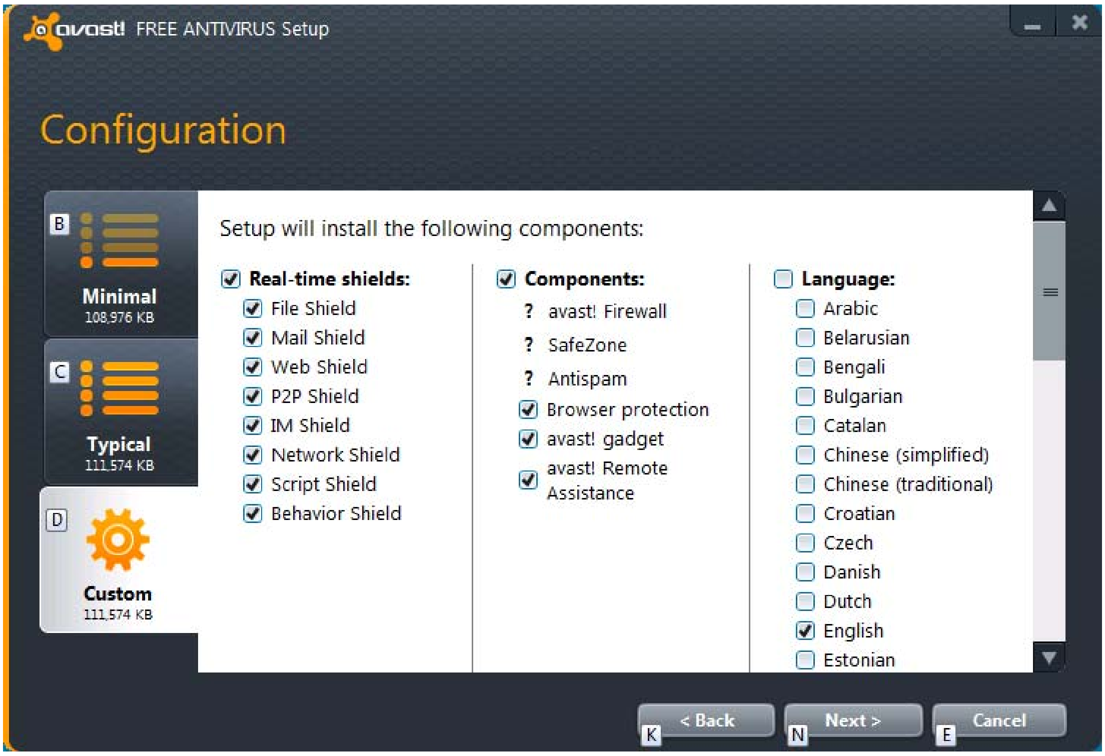
In the case of two programs which are known to rely significantly on cloud access for malware detection (Panda Cloud Antivirus Free and Webroot SecureAnywhere), we performed an additional test to see how these programs react to malware when an Internet connection is not available. We stress that this is not a detection test, but determines whether the programs provide any warning if their malware detection capabilities are reduced when offline.

Outstanding features

In this section, we have pointed out the best individual features we have found in all the programs reviewed.

G Data and **Kaspersky** both provide a full installation file that checks for a more recent version and downloads it if available. This combines the advantages of a full installer and a downloader file.

The setup wizards of **Avast**, **AVG**, **Avira**, **G Data** and **McAfee** offer the user a complete choice of the components to be installed, so that anyone who wants to use Windows Firewall or a third-party antispam program can do so.



Setup will install the following components:

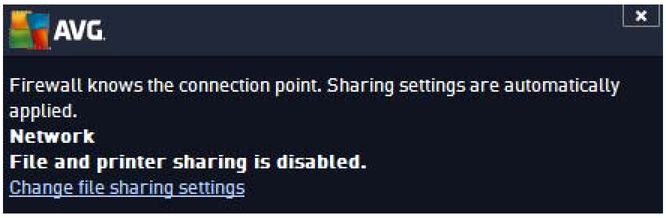
☑ **Real-time shields:**
- ☑ File Shield
- ☑ Mail Shield
- ☑ Web Shield
- ☑ P2P Shield
- ☑ IM Shield
- ☑ Network Shield
- ☑ Script Shield
- ☑ Behavior Shield

☑ **Components:**
- ? avast! Firewall
- ? SafeZone
- ? Antispam
- ☑ Browser protection
- ☑ avast! gadget
- ☑ avast! Remote Assistance

□ **Language:**
- □ Arabic
- □ Belarusian
- □ Bengali
- □ Bulgarian
- □ Catalan
- □ Chinese (simplified)
- □ Chinese (traditional)
- □ Croatian
- □ Czech
- □ Danish
- □ Dutch
- ☑ English
- □ Estonian

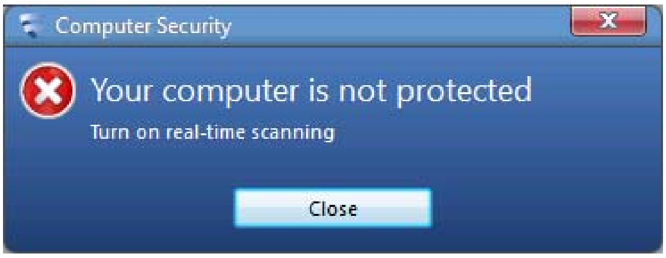
Multilingual families and small businesses will be pleased to see that **Avast** and **AVG** can both install multiple languages, allowing users to quickly change the interface language from the program's options.

The firewalls of **AVG** and **McAfee** both harmonise with the network type (Home/Work/Public) set in Windows Network and Sharing Center, meaning that they are always correctly configured without the user having to make additional changes to the security suite.



Firewall knows the connection point. Sharing settings are automatically applied.
Network
File and printer sharing is disabled.
Change file sharing settings

F-Secure, Kaspersky and **Trend Micro** provide very obvious pop-up warnings, in addition to Windows Action Center's, if real-time protection is disabled.



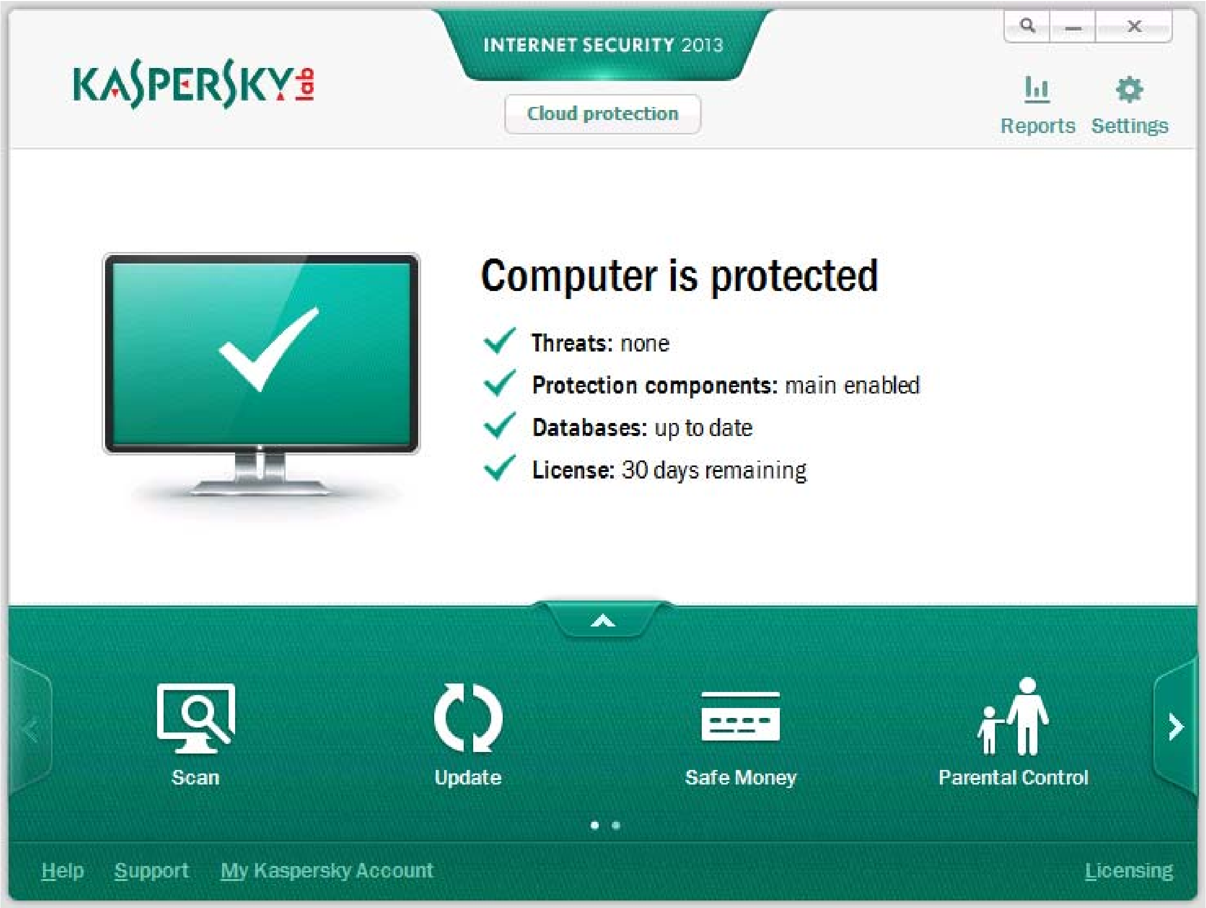
Computer Security

Your computer is not protected

Turn on real-time scanning

The uninstaller programs of **Avast** and **AVG** provide extensive options. Both allow the software to be updated or repaired, and individual components and languages to be added or removed, in addition to deinstallation.

ESET, **Kaspersky**, **Microsoft** and **Trend Micro** have created clear, uncluttered program windows which nonetheless display all essential information and functions, such as a status display, Fix-All button or similar, scan button, help, plus update button and subscription information where applicable.

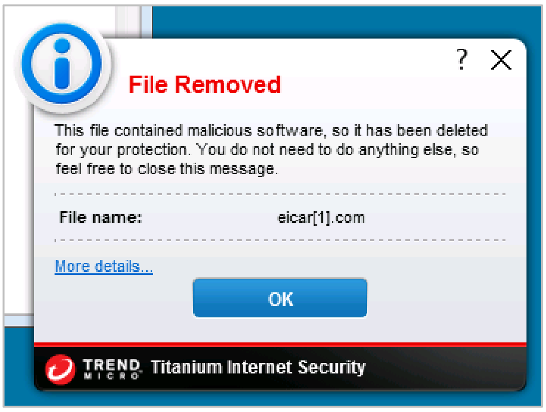


Computer is protected

- **Threats:** none
- **Protection components:** main enabled
- **Databases:** up to date
- **License:** 30 days remaining

The date and time of the next scheduled scan are displayed on the program windows of **Fortinet**, **McAfee**, **Microsoft** and **GFI VIPRE**.

AVG, **F-Secure**, **McAfee** and **Trend Micro** take sensible default actions when malware is discovered, and inform the user clearly whether any further action is required.



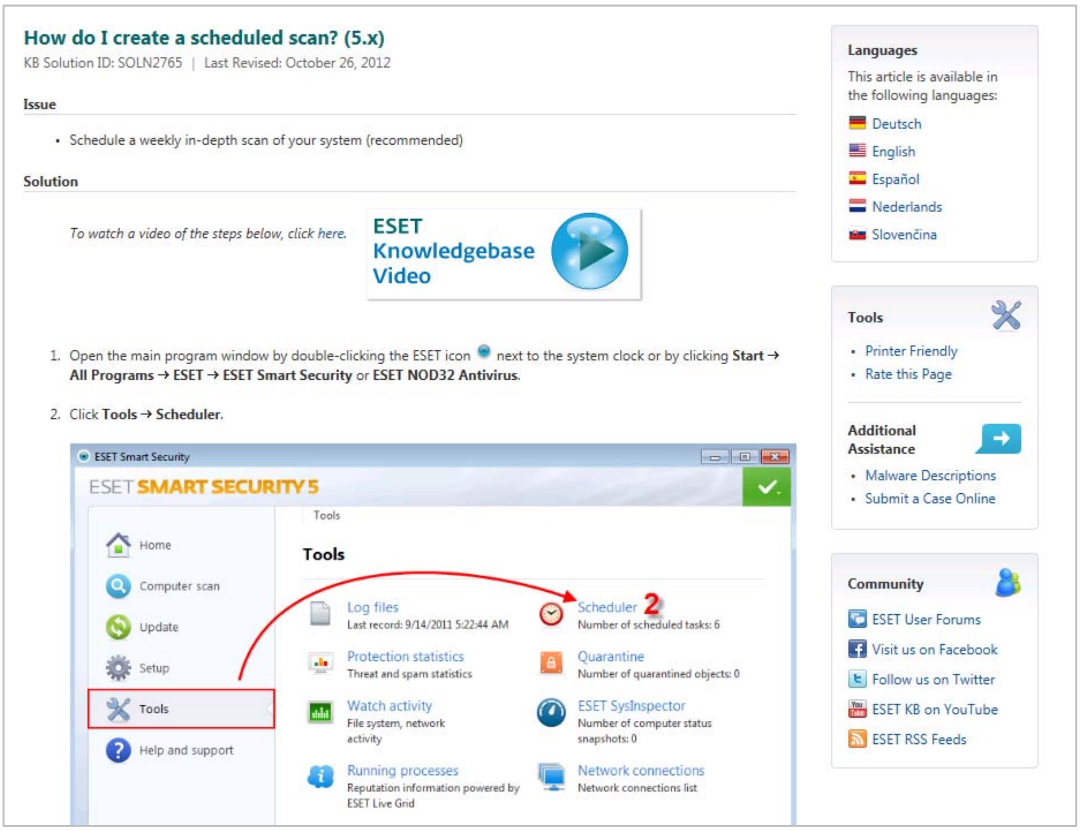
File Removed

This file contained malicious software, so it has been deleted for your protection. You do not need to do anything else, so feel free to close this message.

File name: eicar[1].com

When the PC is started in Safe Mode with Networking, **BullGuard**, **McAfee** and **GFI VIPRE** are all able to update malware signatures, while **Webroot** can connect to the cloud and provide real-time protection.

The help functions and documentation provided by **AVG** and **ESET** are outstanding. Both have local and online help services and downloadable manuals that can only be described as exemplary.



How do I create a scheduled scan? (5.x)

KB Solution ID: SOLN2765 | Last Revised: October 26, 2012

Issue

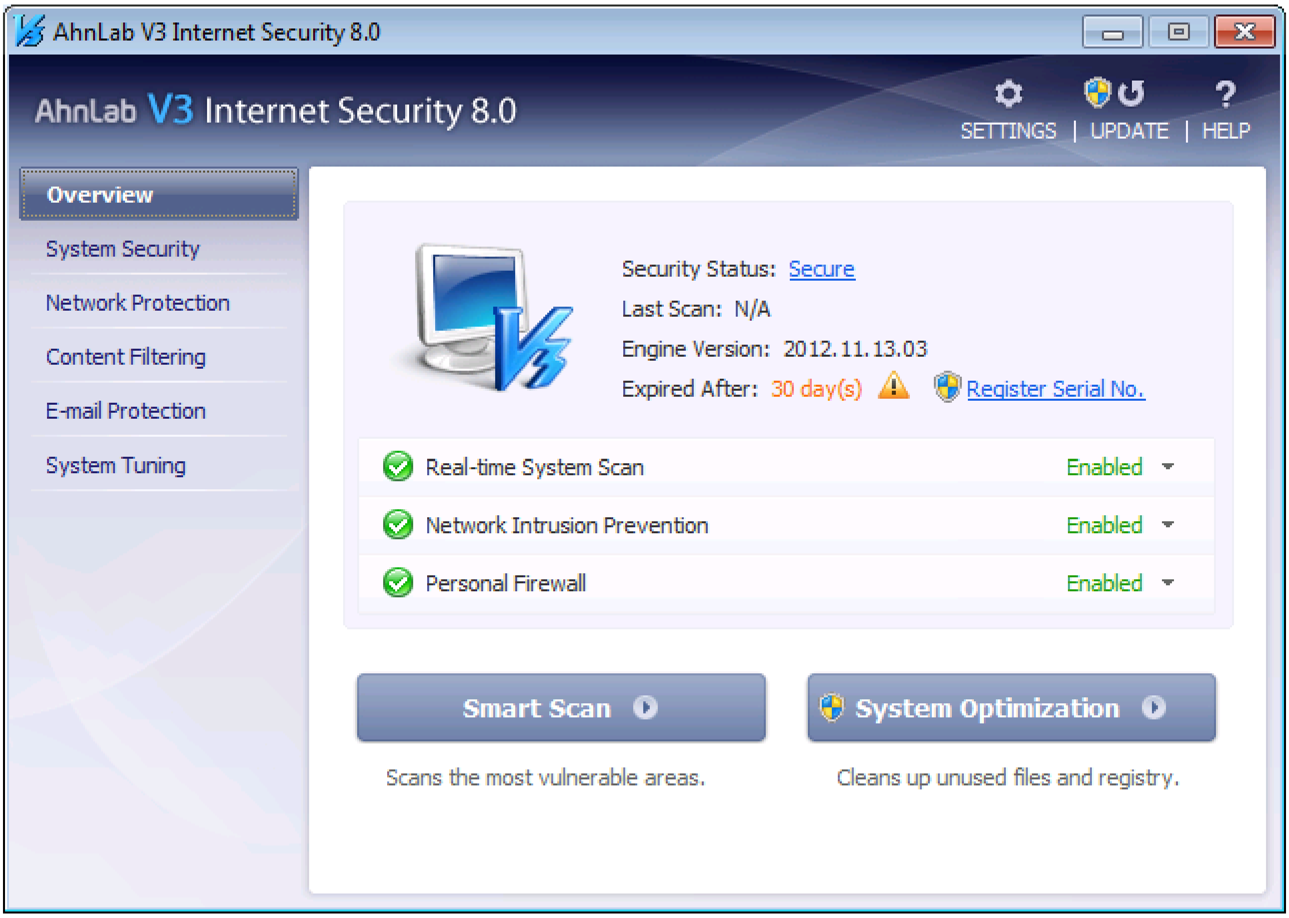
- Schedule a weekly in-depth scan of your system (recommended)

Solution

To watch a video of the steps below, click here.

1. Open the main program window by double-clicking the ESET icon next to the system clock or by clicking **Start → All Programs → ESET → ESET Smart Security** or **ESET NOD32 Antivirus**.
2. Click **Tools → Scheduler**.

AhnLab V3 Internet Security 8.0



AhnLab V3 Internet Security 8.0

Security Status: Secure
Last Scan: N/A
Engine Version: 2012.11.13.03
Expired After: 30 day(s)

Real-time System Scan Enabled
Network Intrusion Prevention Enabled
Personal Firewall Enabled

Scans the most vulnerable areas.
Cleans up unused files and registry.

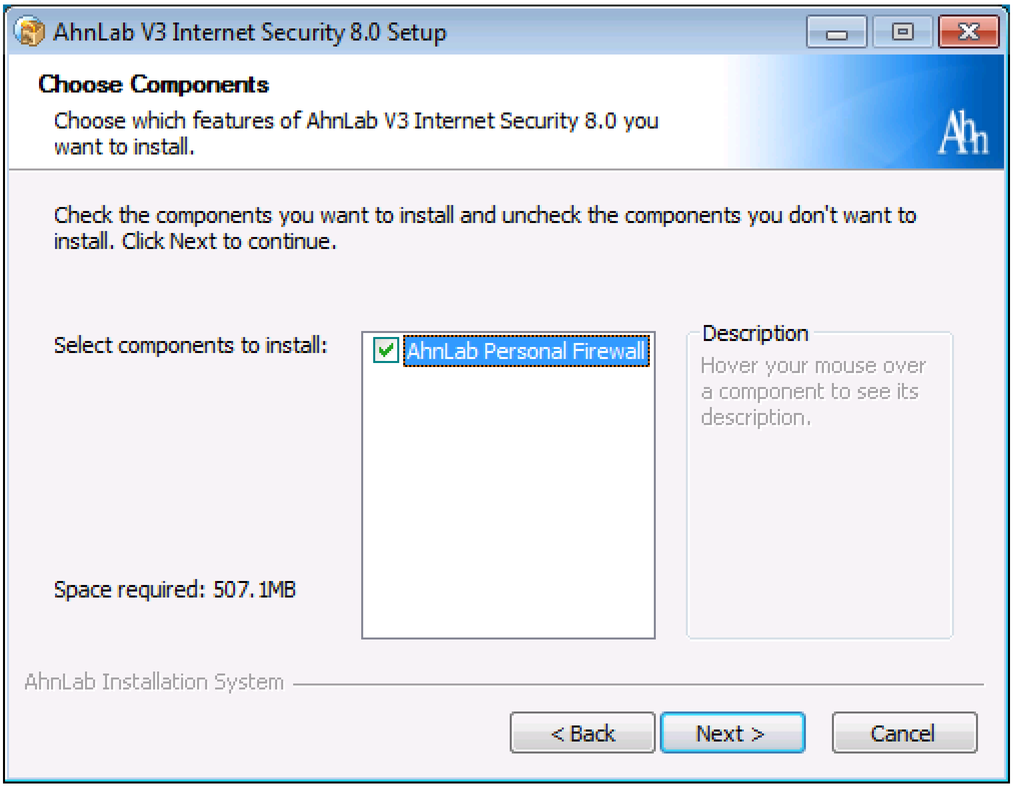
Components

AhnLab V3 Internet Security 8.0 features an antimalware component with email scanning, spam protection, and a firewall. It also boasts system optimisation and secure deletion features.

Installation

We downloaded a 140-MB full installer from the AhnLab website, which is offered as a trial version. Setup is very quick and simple, with few steps. We had the choice of entering a licence key for the full version, or leaving the box blank to use the trial version.

There is the option of installing the AhnLab Personal Firewall, or not:



AhnLab V3 Internet Security 8.0 Setup

Choose Components

Choose which features of AhnLab V3 Internet Security 8.0 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install: ☑ AhnLab Personal Firewall

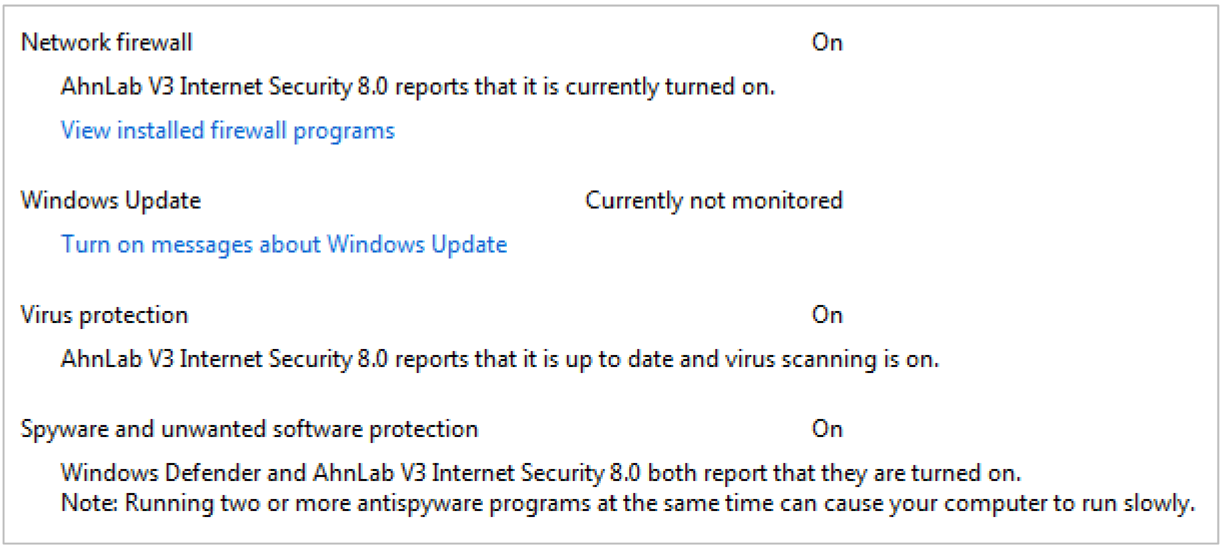
Description
Hover your mouse over a component to see its description.

Space required: 507.1MB

AhnLab Installation System

There is also the choice of folder location. There were no other options, and the setup wizard was finished in about a minute. We were prompted to update the program after installation. A reboot was not required.

AhnLab V3 Internet Security 8 registers itself in Windows Action Center as an antivirus and antispyware program and firewall:



Network firewall On

AhnLab V3 Internet Security 8.0 reports that it is currently turned on.

View installed firewall programs

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

AhnLab V3 Internet Security 8.0 reports that it is up to date and virus scanning is on.

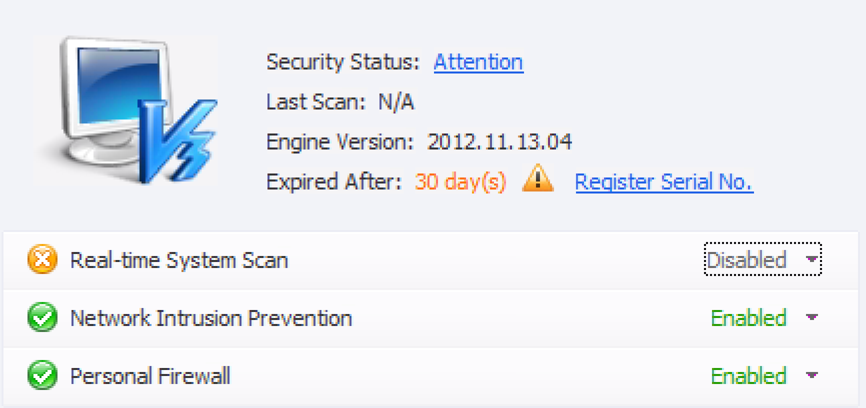
Spyware and unwanted software protection On

Windows Defender and AhnLab V3 Internet Security 8.0 both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

Windows Firewall is disabled, but Windows Defender is not. If AhnLab's real-time protection is disabled, Windows Security Center immediately shows its normal alert. The uninstaller does not offer any options other than complete removal.

Program interface

AhnLab V3 Internet Security 8's main program window consists of a left-hand menu column, and a larger main pane on the right. The title bar also includes Settings, Update and Help buttons. There is an overall status display, although this is only in the form of one word in small text at the top of the main pane, reading either "Secure" or "Attention". There are also status lines for 3 of the individual components, namely Real-time System Scan, Network Intrusion Prevention, and Personal Firewall; each of these has a little tick (checkmark) icon on green if it is activated, or a cross on yellow if not:



Security Status: Attention
Last Scan: N/A
Engine Version: 2012.11.13.04
Expired After: 30 day(s) ⚠ Register Serial No.

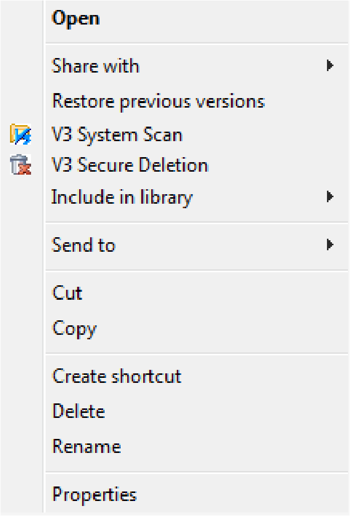
☒ Real-time System Scan — Disabled ▾
✓ Network Intrusion Prevention — Enabled ▾
✓ Personal Firewall — Enabled ▾

Each of the individual components also has its own mini-menu, with which it can be activated or deactivated. The one word representing the status display forms a link to the Protection Settings dialog box, from which all components can be switched on or off.

There is a Smart Scan button on the home page, along with the useful explanation "Scans the most vulnerable areas". Further scan options, including full, custom and scheduled scans, can be found by clicking the less-intuitively named System Security menu on the left.

Subscription information is displayed on the Overview (home) page under the system status.

AhnLab Internet Security integrates itself into Windows Explorer's context menu by means of System Scan and Secure Deletion entries:



Default configuration

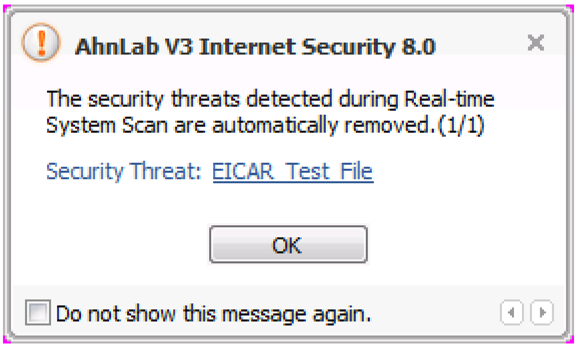
Non-administrator access

When we logged on to our test PC with a non-administrator account, we were able to deactivate the real-time protection without any sort of hindrance. We feel that this is not ideal, especially for a family PC.

Scanning and malware discovery

A scheduled scan is not set by default, but there is a link to the scheduler on the System Security page. We could not find any means of running a boot-time scan.

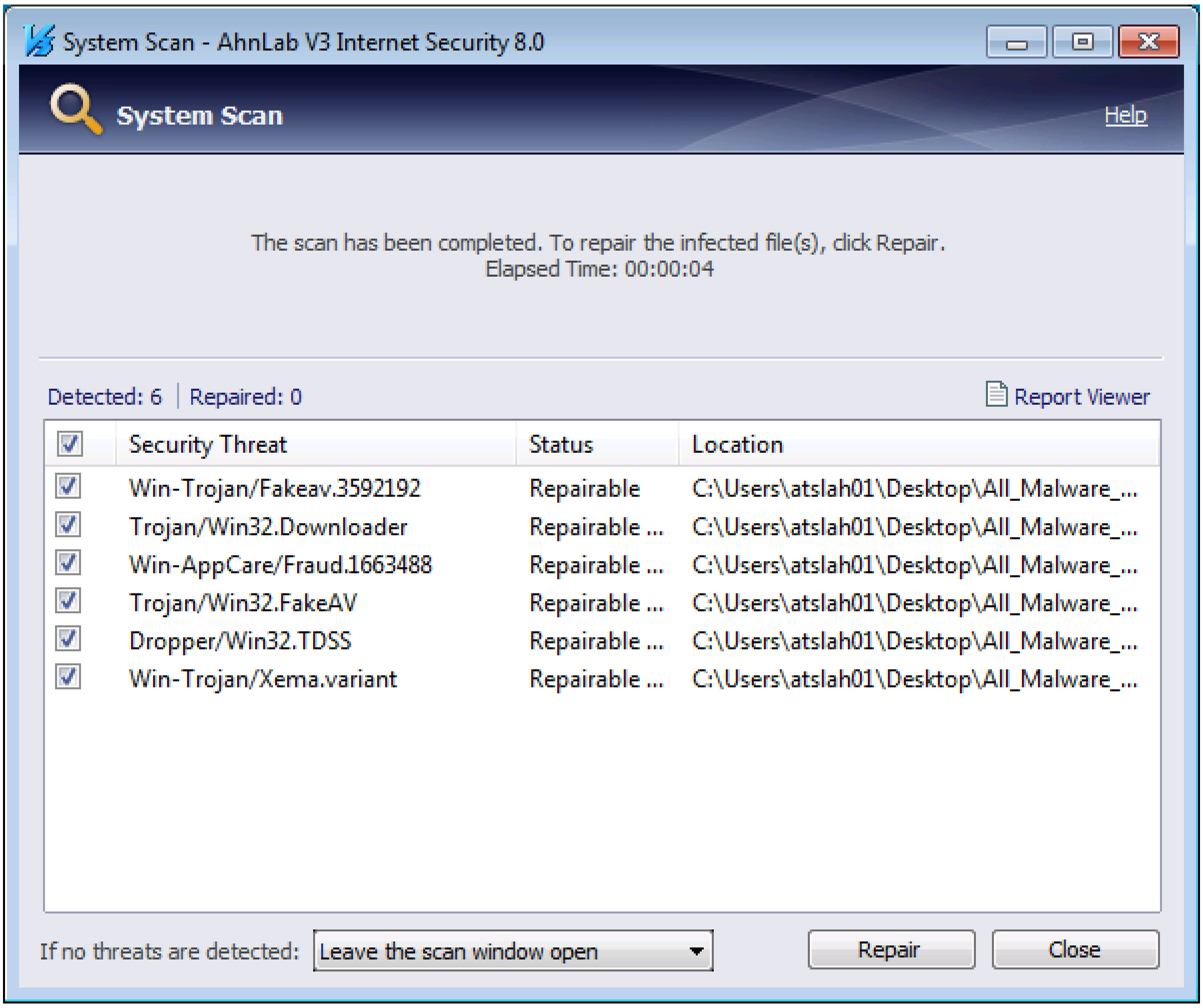
When we attempted to download the EICAR test file, AhnLab Internet Security blocked the download and displayed the warning message shown below; we felt that the wording could be improved, e.g. "have been" rather than "are".


AhnLab V3 Internet Security 8.0

The security threats detected during Real-time System Scan are automatically removed.(1/1)

Security Threat: EICAR_Test_File

The suite reacts in the same way when malware is discovered locally by the real-time protection. Running a custom or context-menu scan on our folder of malware produced the following dialog box, which shows all the items found and allows them to be removed with a click on Repair:



System Scan - AhnLab V3 Internet Security 8.0

System Scan

The scan has been completed. To repair the infected file(s), click Repair.
Elapsed Time: 00:00:04

Detected: 6 | Repaired: 0

☑	Security Threat	Status	Location
☑	Win-Trojan/Fakeav.3592192	Repairable	C:\Users\atslah01\Desktop\All_Malware_...
☑	Trojan/Win32.Downloader	Repairable ...	C:\Users\atslah01\Desktop\All_Malware_...
☑	Win-AppCare/Fraud.1663488	Repairable ...	C:\Users\atslah01\Desktop\All_Malware_...
☑	Trojan/Win32.FakeAV	Repairable ...	C:\Users\atslah01\Desktop\All_Malware_...
☑	Dropper/Win32.TDSS	Repairable ...	C:\Users\atslah01\Desktop\All_Malware_...
☑	Win-Trojan/Xema.variant	Repairable ...	C:\Users\atslah01\Desktop\All_Malware_...

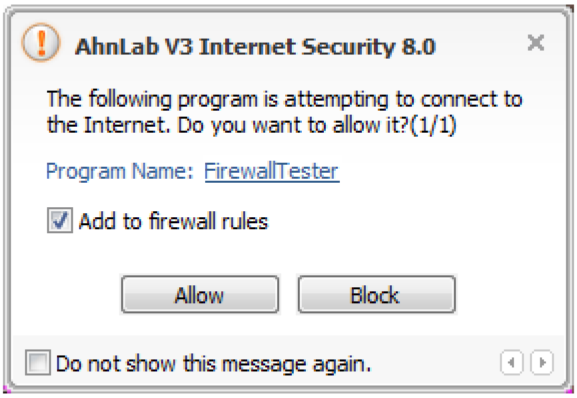
If no threats are detected: Leave the scan window open

Inbound firewall settings

After installation, we found that we could ping our test PC, reach its file share and access it by Remote Desktop, just as before. We note that the AhnLab's firewall mode had been set to "Office", which would appear to be the equivalent of Windows' "Work" setting. We then tried all the other available firewall modes, including "Mobile (Wireless LAN)", and were alarmed to discover that none blocked file sharing or Remote Desktop access on our test PC. Changing the network type to Public in Windows' Network and Sharing Center also had no effect. We are concerned that this could leave a computer open to unauthorised network access, and urge AhnLab to investigate this. We would suggest that users of AhnLab V3 Internet Security who need to prevent any outside access to their PCs via the network should disable the AhnLab firewall and switch on Windows Firewall instead.

Outbound firewall/application control

When we ran our firewall testing program, AhnLab Internet Security displayed the following dialog box, asking whether to allow the program access to the Internet:



AhnLab V3 Internet Security 8.0

The following program is attempting to connect to the Internet. Do you want to allow it?(1/1)

Program Name: FirewallTester

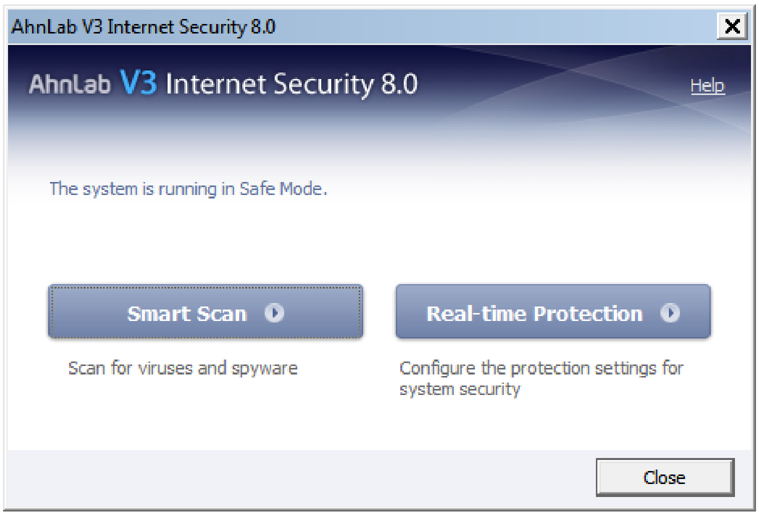
☑ Add to firewall rules

□ Do not show this message again.

We feel that best default setting is not to ask users whether to allow outgoing processes, as non-expert users will probably have no idea whether to allow a process or not. Whilst most Internet security suites allow such queries to be switched on and off, we were unable to find a mode in AhnLab Internet Security which would simply allow the firewall tester to complete its test without asking. Even "Direct (No Firewall)" would not allow this. We note that the Application Control is switched off by default, so it was not this feature that was causing the prompt to be displayed. Only switching AhnLab's firewall off completely allowed the firewall testing program to complete its task without hindrance or query. We feel this inability to switch off queries about outgoing processes could be very frustrating for some people. Again, we are inclined to suggest that users may prefer to switch off the AhnLab firewall and use Windows Firewall instead.

Safe Mode

When we started our test PC in Safe Mode with Networking and tried to open AhnLab Internet Security, the following dialog box was displayed:



AhnLab V3 Internet Security 8.0

The system is running in Safe Mode.

Scan for viruses and spyware

Configure the protection settings for system security

We were pleased to see that the program recognises that it is running in Safe Mode, and found the Smart Scan button obviously useful. We were a little surprised by the Real-time Protection button, as the RTP does not work in Safe Mode; it could only be used to change settings to reactivate RTP when the computer restarts in standard mode.

We were able to run a context-menu scan on our folder of malware, which removed all the items exactly as it would in standard mode. We were unable to find any means of updating signatures, however.

Help and documentation

There is a comprehensive, 120-page manual for AhnLab V3 Internet Security 8 available for download on the AhnLab website. It has been very professionally produced, with all sections accessible with one click from the contents page or Adobe Reader's bookmarks bar. The manual covers system requirements, installation, configuration and maintenance. It has been logically organised and well written. Our one suggestion for improvement would be to put in more screenshots, as there are only a handful in the entire manual.

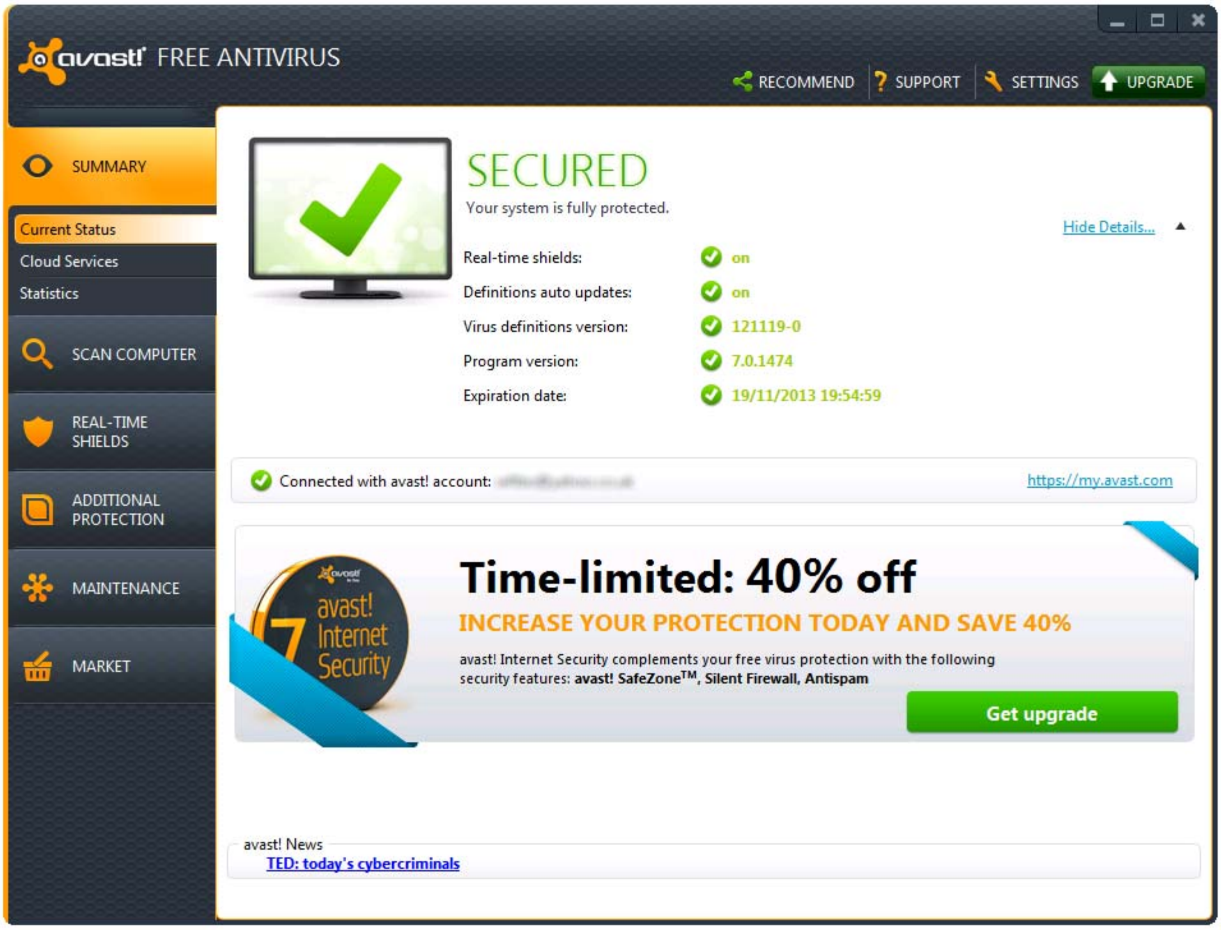
Clicking the Help button on the program window opens the online help function in a browser window (there is no local help function). The content appears to be identical to that of the manual, although broken down into individual pages, with an index pane on the left, and a search function. We were quickly able to find answers to our queries on scheduling a scan and setting scan exceptions.

We also found an FAQ section for AhnLab V3 Internet Security 8 on the website. In contrast to the manual and online help function, we felt that this section had not been well organised, and one particular question/answer combination was very badly written and made no sense at all. We would encourage AhnLab to bring this up to the excellent standard of their other documentation.

Verdict

We found AhnLab V3 Internet Security 8 to have a clear, modern interface that makes important information and functions easy to access. The antimalware component is easy to use, and the manual is outstanding. We do however have concerns about the firewall, particularly its ability to prevent unauthorised access to the PC over the network. We would encourage AhnLab to address this urgently, and suggest that users of the product may currently be best advised to disable the suite's firewall and use Windows Firewall instead.

avast! Free Antivirus 7



SECURED

Your system is fully protected.

Real-time shields: on

Definitions auto updates: on

Virus definitions version: 121119-0

Program version: 7.0.1474

Expiration date: 19/11/2013 19:54:59

Connected with avast! account: [redacted] https://my.avast.com

Time-limited: 40% off

INCREASE YOUR PROTECTION TODAY AND SAVE 40%

avast! Internet Security complements your free virus protection with the following security features: **avast! SafeZone^{TM}, Silent Firewall, Antispam**

avast! News

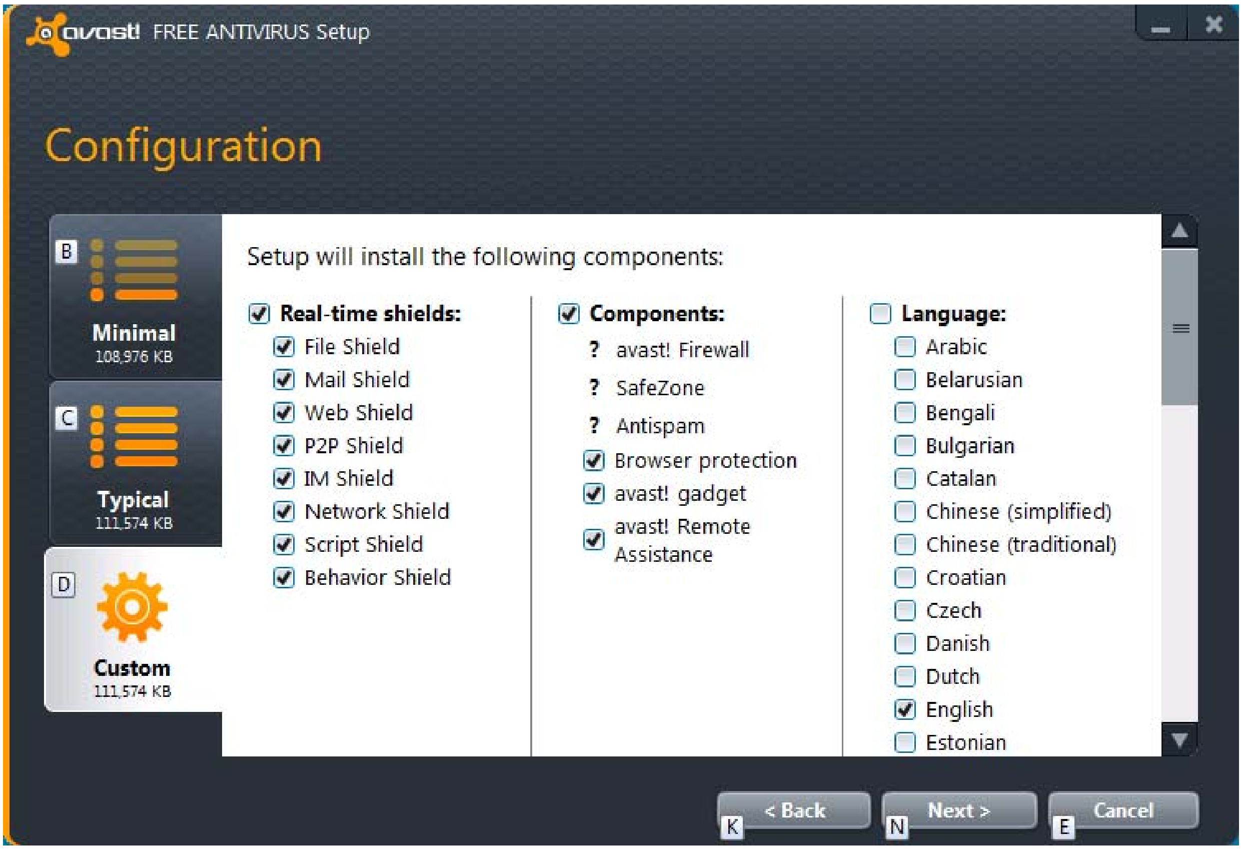
TED: today's cybercriminals

Components

Avast! Free Antivirus 7 is an antivirus and antispyware program with email scanner.

Installation

We installed the suite from the 93 MB full installer file provided for trial use. The setup wizard provides the option to install the Google Chrome browser (we declined), and Express and Custom Install options; we chose the latter. Steps included the choice of installation folder and a full choice of components and interface languages. We were pleased to see that avast's multi-language selection still includes the humorous "Pirate Talk". We note that clicking the components marked with a question mark (avast! Firewall, SafeZone and Antispam) opens up a web page advertising the paid-for avast! Internet Security Suite; these three features are not included in avast! Free Antivirus.



Configuration

Minimal 108,976 KB

Typical 111,574 KB

Custom 111,574 KB

Setup will install the following components:

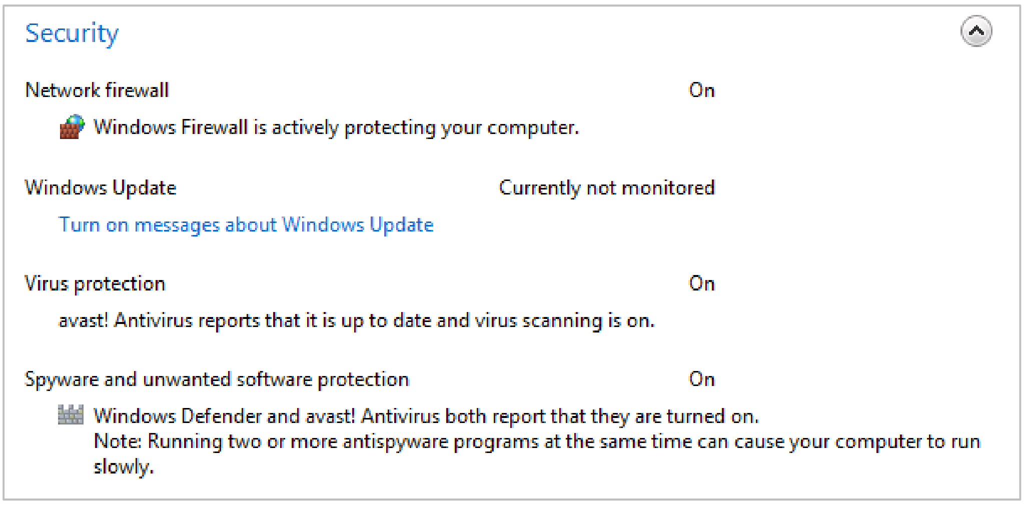
☑ **Real-time shields:**
- ☑ File Shield
- ☑ Mail Shield
- ☑ Web Shield
- ☑ P2P Shield
- ☑ IM Shield
- ☑ Network Shield
- ☑ Script Shield
- ☑ Behavior Shield

☑ **Components:**
- ? avast! Firewall
- ? SafeZone
- ? Antispam
- ☑ Browser protection
- ☑ avast! gadget
- ☑ avast! Remote Assistance

□ **Language:**
- □ Arabic
- □ Belarusian
- □ Bengali
- □ Bulgarian
- □ Catalan
- □ Chinese (simplified)
- □ Chinese (traditional)
- □ Croatian
- □ Czech
- □ Danish
- □ Dutch
- ☑ English
- □ Estonian

At the end of the installation process, the user is required to register the program by entering a name and email address. A reboot is not needed.

Avast! Free Antivirus 7 registers itself as an antivirus and antispyware program in Windows 7's Action Center. Windows Defender is not disabled.



Security

Network firewall On

Windows Firewall is actively protecting your computer.

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

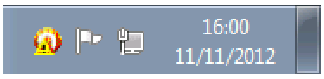
avast! Antivirus reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

Windows Defender and avast! Antivirus both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

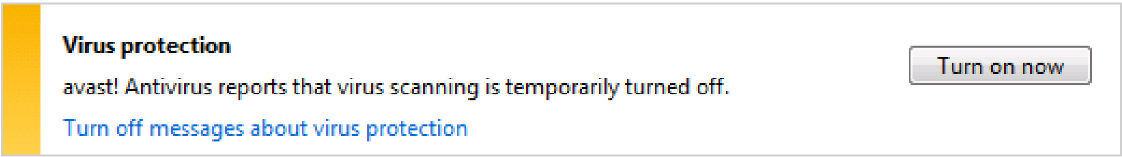
When we disabled real-time protection (choosing the "Permanently" option in avast's settings), Windows Action Center produced only a very muted warning, compared to the standard warning made when the system's antivirus program is turned off.

There is no warning message or changed Action Center icon visible in the system tray (although the avast! icon itself does change):



avast! system tray icons

Additionally, the warning message in the Action Center window is yellow rather than red, and reports that avast! is "temporarily" turned off (despite our deliberately selecting "permanently" when disabling the RTP):



Virus protection

avast! Antivirus reports that virus scanning is temporarily turned off.

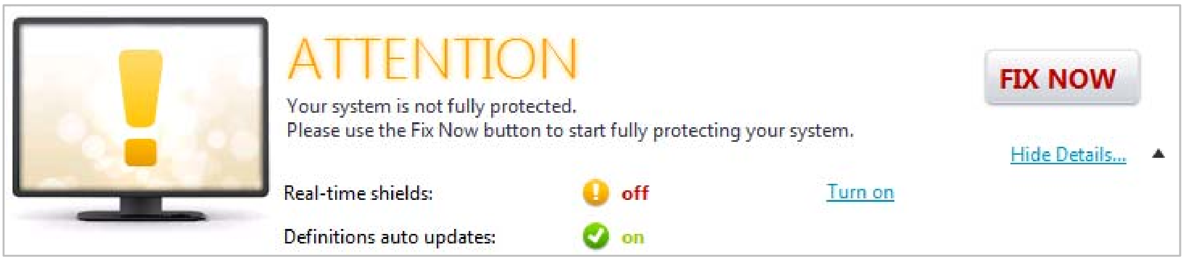
avast! Action Center warning

We feel that the muted warning from Windows Action Center is much less obvious than the standard warning message, and would not be apparent to users unless they deliberately checked the Action Center. We would urge avast! to reconsider the suite's interaction with Action Center and implement the standard warning when important protection components are turned off.

Avast's uninstaller options, as in previous versions, are impressive. The uninstall/change wizard can be used to update the program to the latest version, repair the existing installation, add or remove any components and/or interface languages, or simply uninstall the software completely. We regard this as exemplary.

Program interface

The main program window of avast! Free Antivirus 7 retains the familiar layout of previous versions, with a left-hand column of menu buttons, and a big pane to the right of this to show the information/options selected from the menu. There is a big status display, showing the word "Secured" and a tick (checkmark) symbol in green, if all is well. If a protection component is disabled, the wording changes to "Attention" with an exclamation mark in yellow, and a very obvious "Fix Now" button appears. A detailed component status list shows exactly where the problem lies, and provides an additional "Turn on" link:



ATTENTION

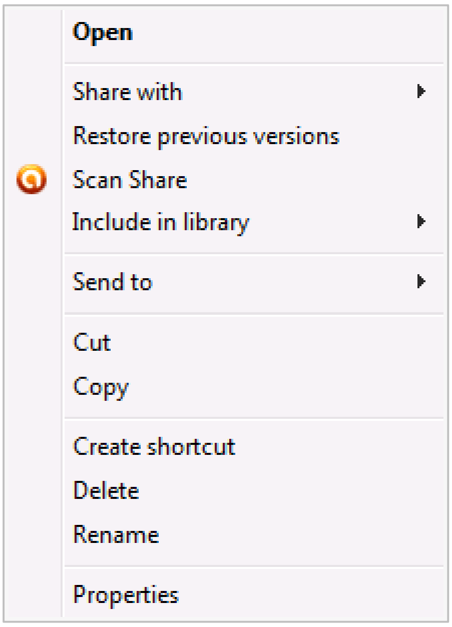
Your system is not fully protected.
Please use the Fix Now button to start fully protecting your system.

Real-time shields: off

Definitions auto updates: on

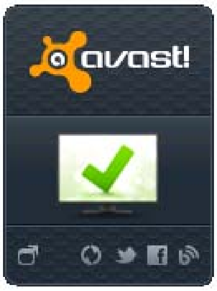
Manually updating the virus signatures is not very obvious, as the word "Update" cannot be seen anywhere in the window. The function can in fact be found by clicking on the Maintenance menu button, and allows the program itself to be updated, as well as the definitions.

The very obvious Scan Computer menu button allows a wide range of scans to be run, including quick, full system, custom and removable media scans. Windows Explorer integration, i.e. additions to the context menu seen when right-clicking a file or folder, is limited to one simple entry, "Scan [foldername]":



As a free program, avast! Free Antivirus does not have a subscription, but has to be registered, as noted above. This is valid for one year, after which the program needs to be re-registered. Registration information is displayed on the Summary (home) page of the program, with more details available in the Registration sub-menu of Maintenance. All the help functions can be registered accessed easily by clicking the Support button at the top of the window.

avast! Free Antivirus 7 provides a desktop gadget for Windows 7/Vista users, which has a status icon and links to the program window and update functions. On our test PC, this was not displayed automatically, but had to be activated by opening the Desktop Gadgets Control Panel applet.



Default configuration

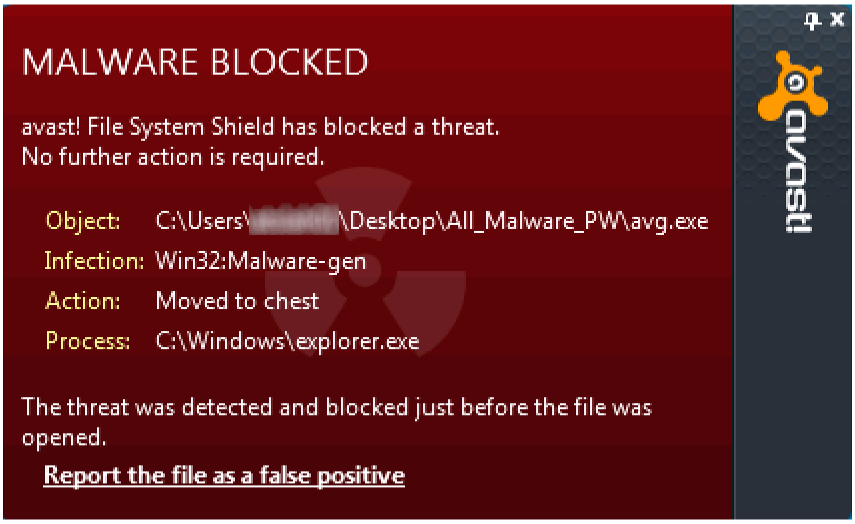
Non-administrator access

We found that we could disable the real-time protection in the avast! program even when logged on to Windows with a standard user account. As happened when using an administrator account, avast's own warning message comes up, but this can be confirmed simply by clicking "OK". We would not regard this as ideal, especially for a family computer.

Scanning and malware discovery

There is no scheduled scan set up by default, but any individual scan can be set to run on a schedule by going into that scan's settings. A boot-time scan can easily be run from the appropriately named sub-menu.

The real-time protection of avast! Free Antivirus 7 reacted to local malware by quarantining it and displaying the following message, which made clear what had happened:



MALWARE BLOCKED

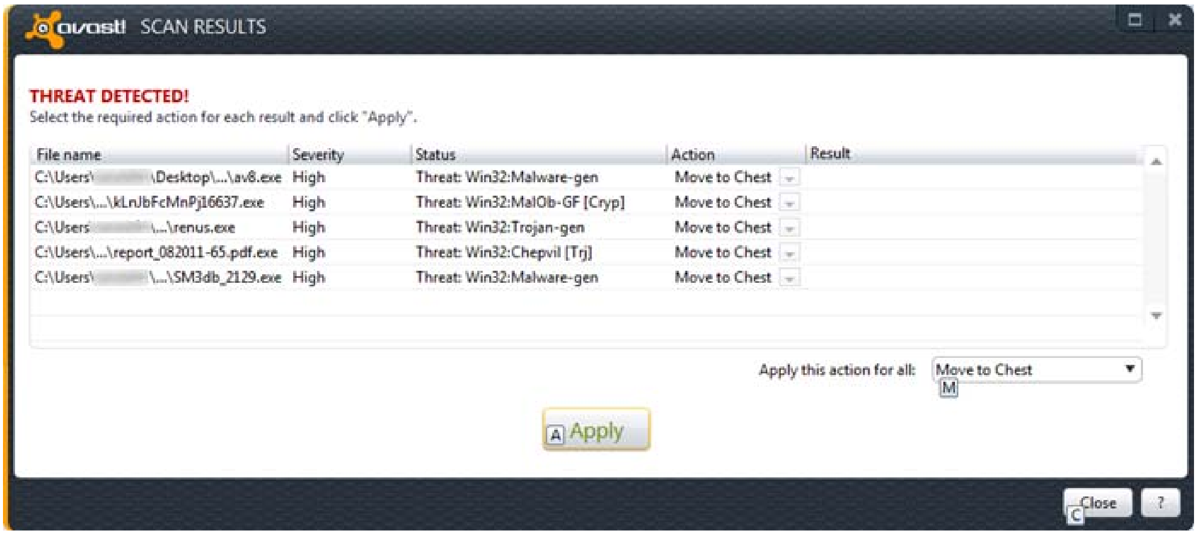
avast! File System Shield has blocked a threat.
No further action is required.

Object: C:\Users\[redacted]\Desktop\All_Malware_PW\avg.exe
Infection: Win32:Malware-gen
Action: Moved to chest
Process: C:\Windows\explorer.exe

The threat was detected and blocked just before the file was opened.

Report the file as a false positive

Scans run from the console or context menu both show that malware has been found, and let the user decide what to do by clicking on "Show Results":

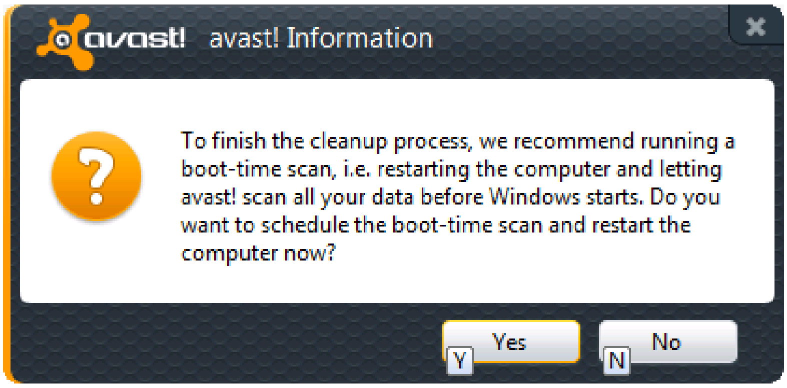


THREAT DETECTED!
Select the required action for each result and click "Apply".

File name	Severity	Status	Action	Result
C:\Users\ [redacted] \Desktop\...\av8.exe	High	Threat: Win32:Malware-gen	Move to Chest	
C:\Users\...\kLnJbFcMnPj16637.exe	High	Threat: Win32:MalOb-GF [Cryp]	Move to Chest	
C:\Users [redacted] \...\renus.exe	High	Threat: Win32:Trojan-gen	Move to Chest	
C:\Users\...\report_082011-65.pdf.exe	High	Threat: Win32:Chepvil [Trj]	Move to Chest	
C:\Users\ [redacted] \...\SM3db_2129.exe	High	Threat: Win32:Malware-gen	Move to Chest	

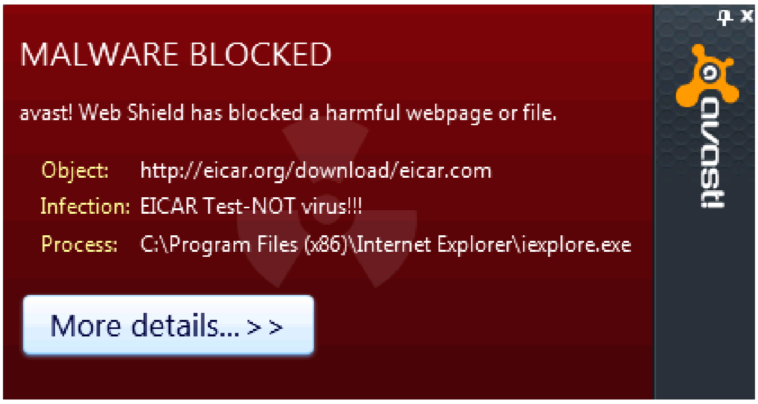
Apply this action for all: Move to Chest

The default action is to quarantine the malware, which can be done very conveniently by clicking Apply. A boot-time scan is recommended; we can only congratulate avast! for being thorough here:



To finish the cleanup process, we recommend running a boot-time scan, i.e. restarting the computer and letting avast! scan all your data before Windows starts. Do you want to schedule the boot-time scan and restart the computer now?

When we attempted to download the EICAR test file, avast! blocked the download and displayed the warning message below; we feel the "No further action is required" line found in the program's other malware warnings would be a nice addition for inexperienced users.



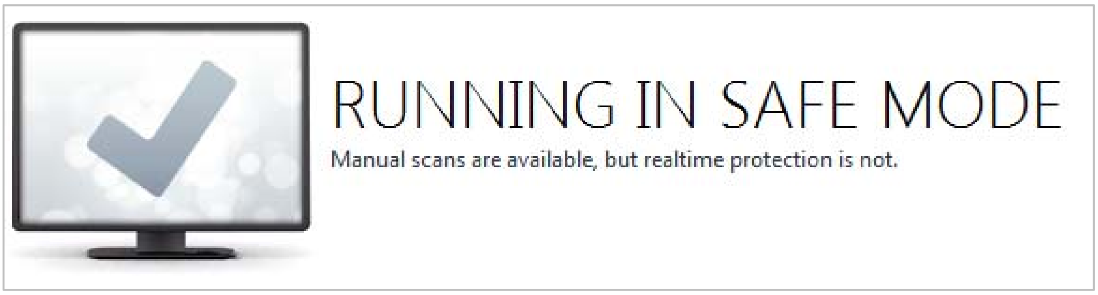
MALWARE BLOCKED

avast! Web Shield has blocked a harmful webpage or file.

Object: http://eicar.org/download/eicar.com
Infection: EICAR Test-NOT virus!!!
Process: C:\Program Files (x86)\Internet Explorer\iexplore.exe

Safe Mode

When we started our test PC in Safe Mode with Networking and opened avast! Free Antivirus 7, it displayed the following message in its status area:



RUNNING IN SAFE MODE

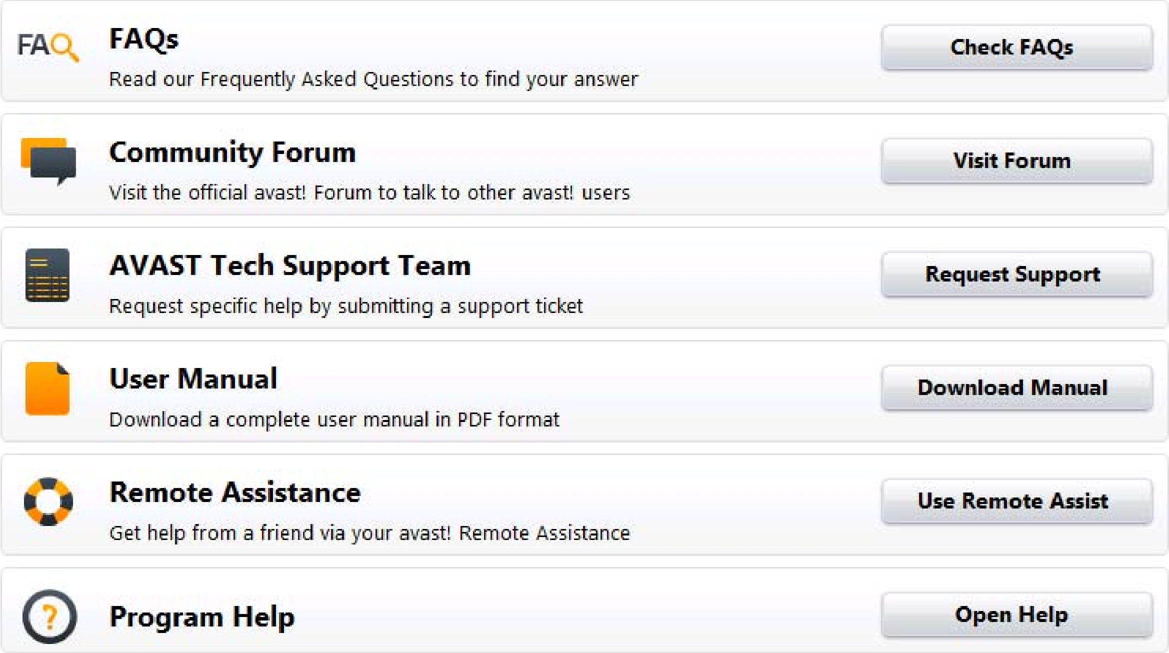
Manual scans are available, but realtime protection is not.

We found this to be an excellent idea, as the user is immediately informed as to what the program can and can't do in Safe Mode. As expected, we were able to run a custom scan of our malware folder, and remove the malware in exactly the same way as in normal mode. All other console scan options would have been available too.

We found that although the update function was not obviously disabled, running it made no progress for over 5 minutes, so we abandoned the attempt.

Help and documentation

The help functions in avast! Free Antivirus 7 are easily accessed by clicking the Support button at the top of the window. An impressively wide range of options is clearly displayed:



FAQs

Read our Frequently Asked Questions to find your answer

Check FAQs

Community Forum

Visit the official avast! Forum to talk to other avast! users

Visit Forum

AVAST Tech Support Team

Request specific help by submitting a support ticket

Request Support

User Manual

Download a complete user manual in PDF format

Download Manual

Remote Assistance

Get help from a friend via your avast! Remote Assistance

Use Remote Assist

Program Help

Open Help

When we searched the (local) Program Help feature, we quickly found articles relating to our queries on scheduling a scan and setting scan exceptions. Unfortunately, in both cases the instructions evidently assume that the user has already found the page concerned, and is wondering what to do with it. There is no indication as to how to navigate to the relevant area of the settings in the first place. For example, the entry on scheduling begins “On this page you can schedule a scan to run once, automatically on a given day…”. We feel that entries such as this rather miss the point of a help service, and question their value to the majority of users. Unfortunately, our search of the online knowledge base failed to find relevant answers either.

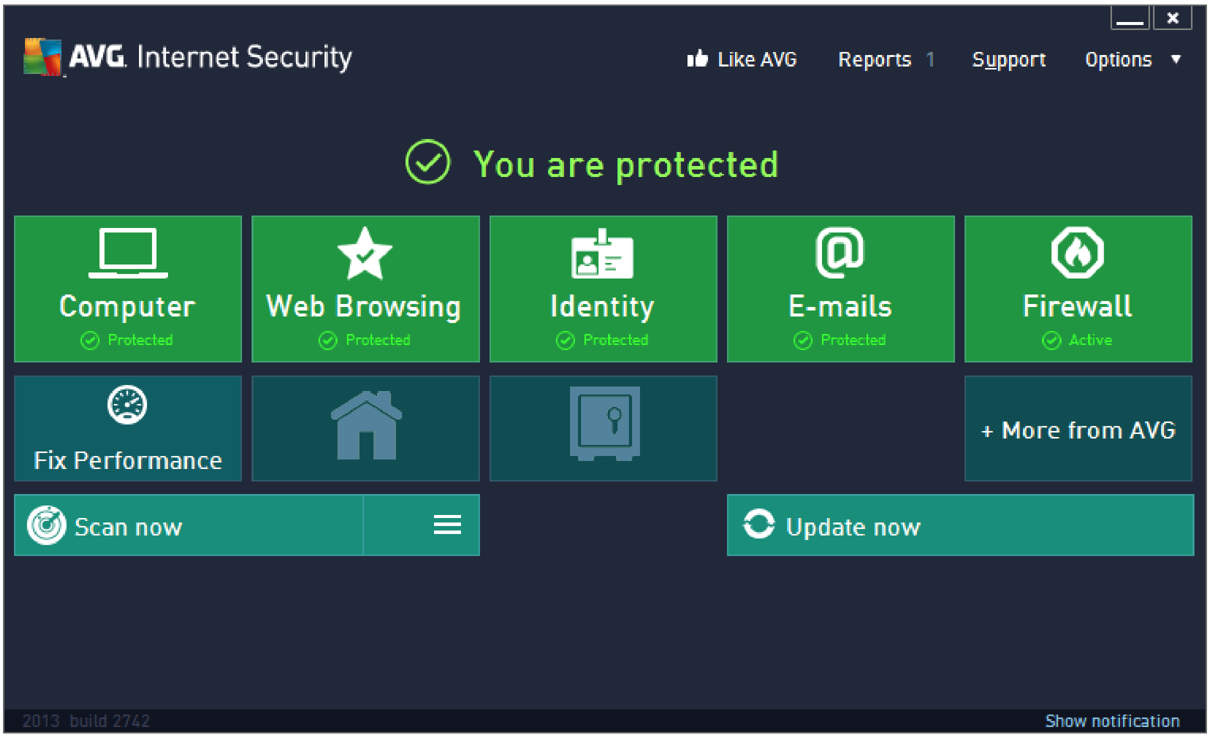
The user manual, which can be downloaded conveniently from the program’s Support page, is entitled “Quick Start Guide”. It is 25 pages long, and as the name suggests, is a brief introduction to the most important aspects of the program, including the default installation process, updating and scanning. It is very well illustrated with screenshots. In terms of content, we would say that it is fine as far as it goes, but that a more detailed manual would be helpful. Whilst we found the simple format of the Quick Start Guide quite acceptable in principle, we were rather left with the impression that the document had been produced in a hurry, with no form of indexing or bookmarking, and slightly blurred-looking text and screenshots even at 100% magnification on a 1600 x 1200 resolution 20” professional -standard monitor. We also note that the manual has been produced in a format that makes text searching impossible; even using the search term *avast!* failed to produce any results in Adobe Reader’s search function.

As a whole, we have to say that we found the help functions and documentation for avast! Free Antivirus 7 to be rather disappointing.

Verdict

We consider avast! Free Antivirus 7 to be an excellent program in many ways. There is an exemplary range of options in the setup and uninstaller wizards, and the program interface is clean and modern, making almost all important functions and information easy to find. It has sensible default configuration, clear and appropriate reactions on malware discovery, and useable scanning options in Safe Mode. However, we feel that communication with Windows Action Center, as well as the help functions, could be improved.

AVG Internet Security 2013



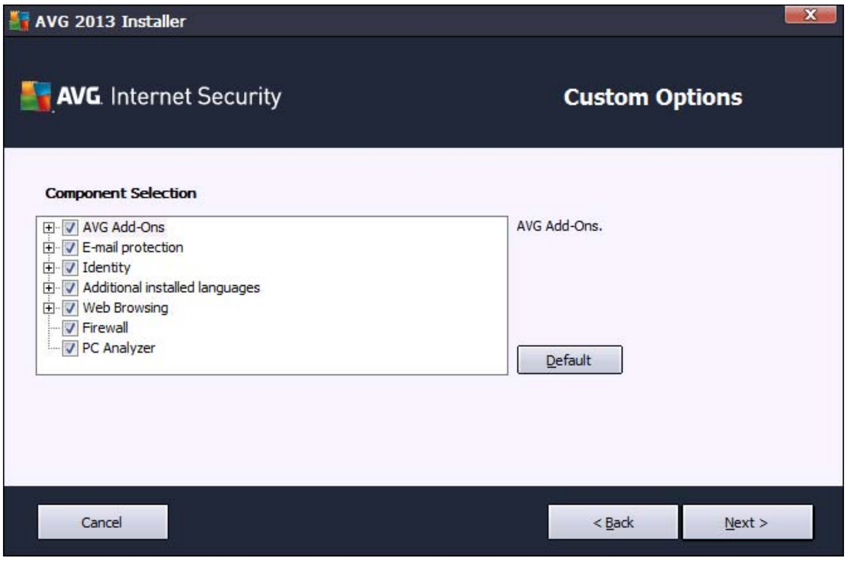
Components

AVG Internet Security 2013 includes an antivirus/antispyware component with integrated email protection, a firewall, and antispam module. There is a web protection component to guard against dangerous websites, and an identity theft module. Parental control is not included, but can be purchased separately.

Installation

For trial use, AVG provides a 4.2 MB online installer (downloader), which downloads a further 53.3 MB of code for a standard installation. We note that a full installation package is available for download from the AVG website. Various European and Asian languages are offered for the setup wizard and user interface. There is an opportunity to insert a purchased licence key if available; the relevant box is pre-filled with a trial key, enabling the product to be used as a 30-day test version if no commercial key is inserted.

There is a choice of Standard and Custom setup types; we chose the latter. This allowed us to choose the location of the setup folder, and provided us with an extensive range of additional interface languages, plus a complete choice of the components to be installed:


AVG 2013 Installer

AVG Internet Security

Custom Options

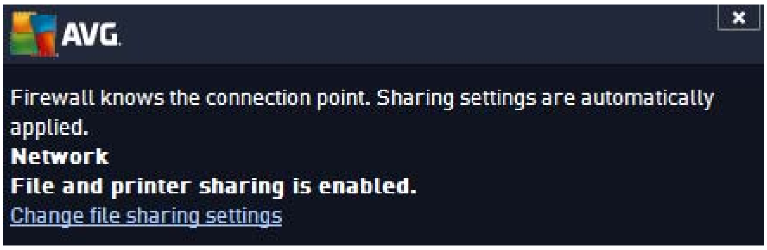
Component Selection

- ☑ AVG Add-Ons
- ☑ E-mail protection
- ☑ Identity
- ☑ Additional installed languages
- ☑ Web Browsing
- ☑ Firewall
- ☑ PC Analyzer

AVG Add-Ons.

There is a further option of installing the AVG browser toolbar and AVG Secure Search. The user is offered the chance to create an AVG account by registering an email address and password, though this is optional.

The setup program does not ask whether the network the computer is connected to is private or public. However, it automatically reads the current Windows settings and configures the suite accordingly:


AVG

Firewall knows the connection point. Sharing settings are automatically applied.

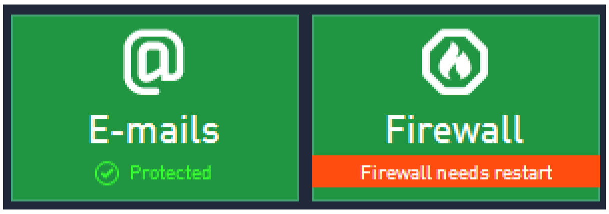
Network

File and printer sharing is enabled.

Change file sharing settings

We would suggest that the phrase “Firewall knows the connection point” is rather unclear and could be improved, e.g. “Private network detected”.

The main program window indicates that a reboot is required for the optimal functioning of the firewall:

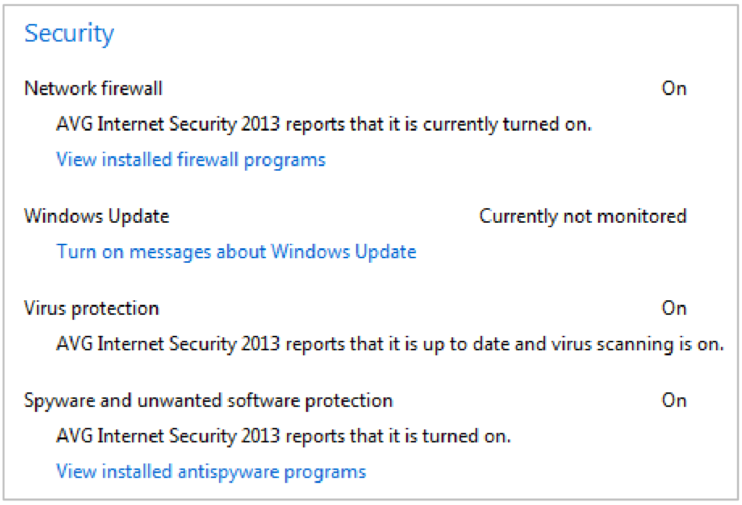

E-mails

Protected

Firewall

Firewall needs restart

AVG Internet Security 2013 registers itself in Windows 7's Action Center as an antivirus and antispyware program and firewall. Windows Defender and Windows Firewall are both switched off:



Security

Network firewall On

AVG Internet Security 2013 reports that it is currently turned on.

View installed firewall programs

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

AVG Internet Security 2013 reports that it is up to date and virus scanning is on.

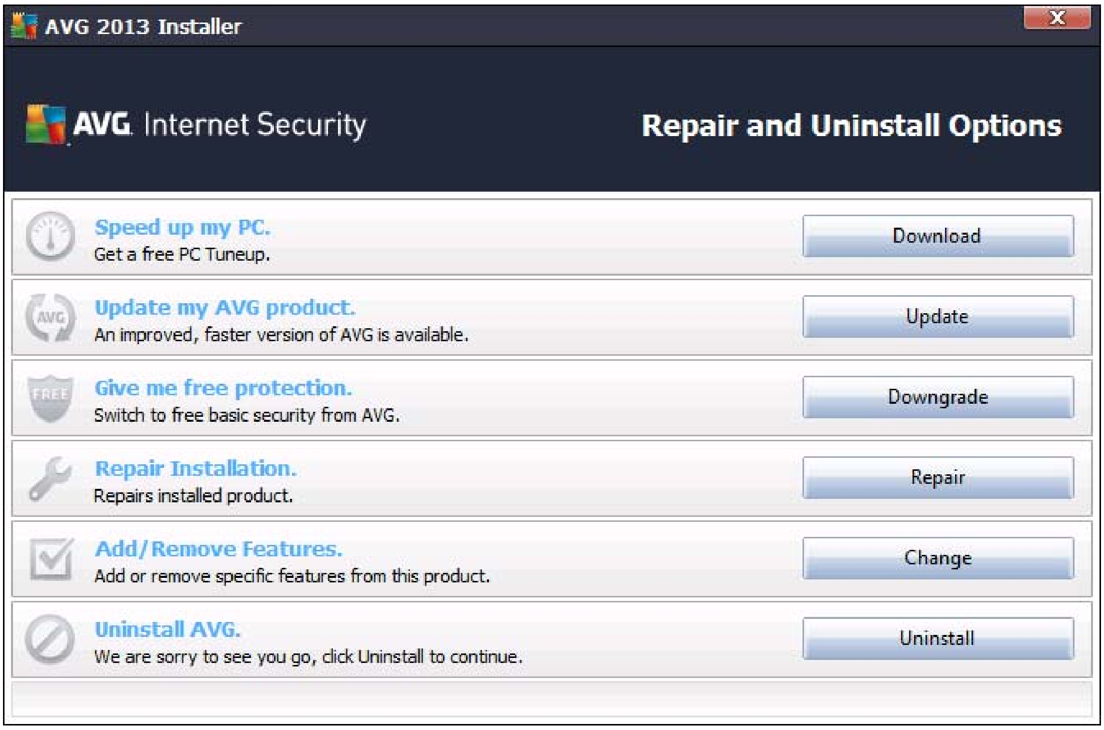
Spyware and unwanted software protection On

AVG Internet Security 2013 reports that it is turned on.

View installed antispyware programs

If AVG's malware protection or firewall components are disabled, this is immediately shown as a warning in Action Center.

The options available in the uninstaller program are very comprehensive, and include updating and repairing the product, plus adding or removing components, as well as removing the program completely. The Add/Remove Features option displays the same component selection dialog box seen in the setup wizard, allowing any individual component or interface language to be added or removed.



AVG 2013 Installer

AVG Internet Security

Repair and Uninstall Options

Speed up my PC.
Get a free PC Tuneup.

Update my AVG product.
An improved, faster version of AVG is available.

Give me free protection.
Switch to free basic security from AVG.

Repair Installation.
Repairs installed product.

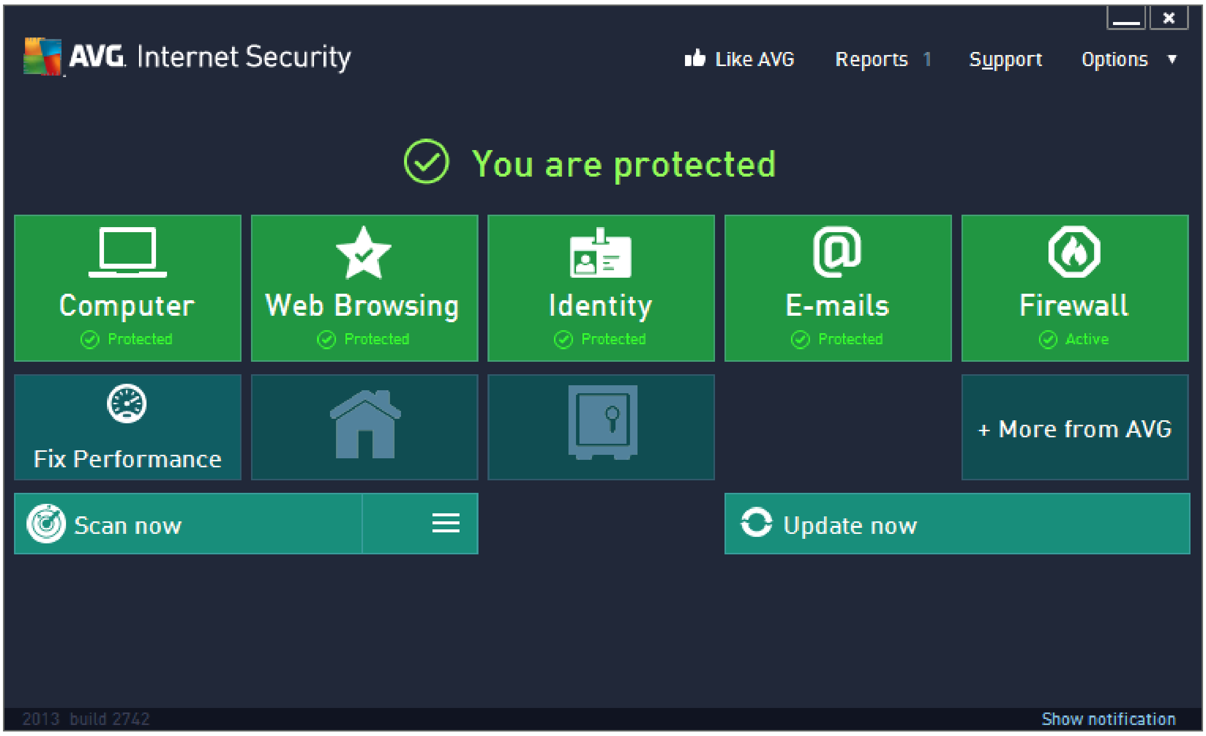
Add/Remove Features.
Add or remove specific features from this product.

Uninstall AVG.
We are sorry to see you go, click Uninstall to continue.

We found AVG's setup process to be very simple and straightforward, but with an excellent range of options available in the custom setup. We particularly liked the ability to select or deselect any component, and choose from a wide range of additional languages, in both the installation and maintenance/uninstaller wizards. We also liked the message informing us that the network type had been discovered and the firewall configured appropriately, even if it was slightly confusing in its wording.

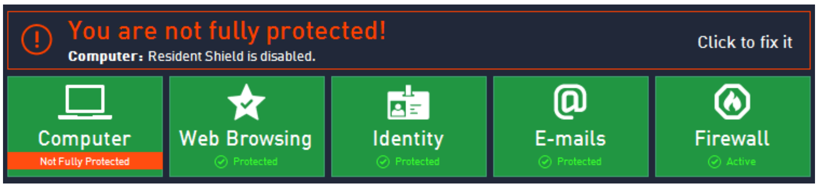
Program interface

The user interface of AVG Internet Security 2013 has been completely redesigned and is now reminiscent of Windows 8's Start Screen, consisting primarily of tile-like buttons in pastel shades with simple white icons.



You are protected

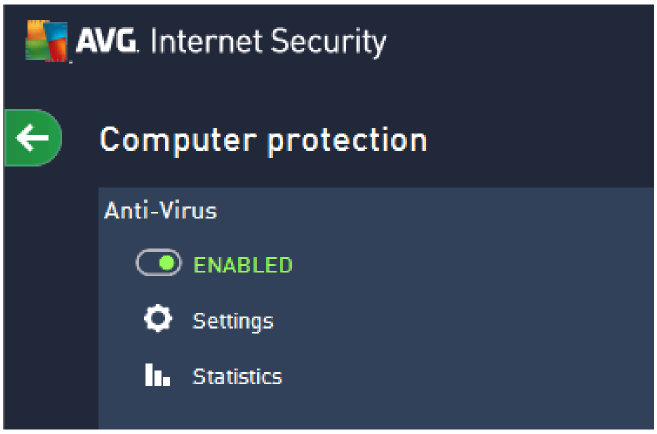
There is a status display near the top of the window; if all is well, this will state "You are protected" in green text, with a tick (checkmark) symbol. Disabling the real-time protection immediately changes the text to "You are not fully protected" in red, with an exclamation mark symbol, and a helpful explanation of the problem ("Resident Shield is disabled") in white text below. A prominent link with the text "Click to fix it" to the right of the warning resolves the problem instantly when clicked.



You are not fully protected!

Computer: Resident Shield is disabled.

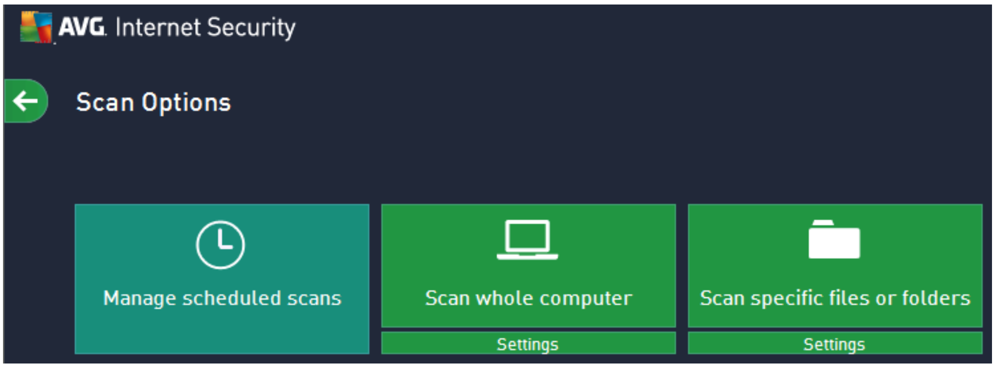
The window is dominated by 5 medium-green tiles in the middle, running left to right, entitled Computer, Web Browsing, Identity, E-Mails and Firewall. Clicking on any of the tiles displays a configuration page for the item in question, with an enable/disable button, settings, and (where appropriate) statistics:



A back arrow allows the user to return to the program's home page.

A second row of slightly smaller tiles in a dark turquoise colour could be fairly described as advertising, as each links to a page giving details of other AVG components or products, such as Family Safety and Mobile Protection, which can be obtained separately.

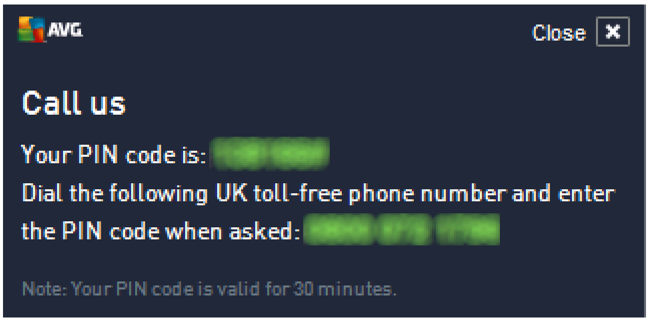
The third row contains just two elongated tiles, entitled Scan Now and Update Now. Scan Now starts a full system scan, whilst the Options section on the right of the button opens a page of scan options, with scheduled, full and custom scans available:



We were unable to find an option to run a boot-time scan.

A discreet menu bar along the top of the window has text links for Reports, Support and Options. Reports shows logs of updates, scans and malware found; Options is a very comprehensive menu, which not only gives access to settings, quarantine and licence information, but also includes duplicate links to scan, update and help functions.

Support opens a page with buttons for telephone support, chat support, FAQs, virus removal, AVG Community, and, in the UK at least, premium support from Virgin Digital Help. The telephone support buttons displays a phone number and PIN code:



Call us

Your PIN code is: [redacted]

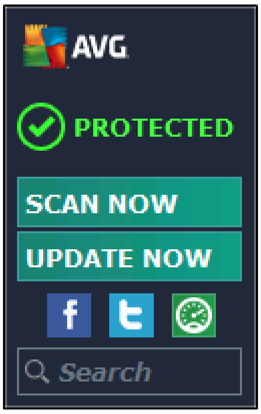
Dial the following UK toll-free phone number and enter the PIN code when asked: [redacted]

Note: Your PIN code is valid for 30 minutes.

Licence information (key number and expiry date) are also shown on the support page.

AVG Internet Security integrates itself discreetly into Windows Explorer by means of a single entry in the context menu (shown when a file or folder is right-clicked), "Scan with AVG".

Users of Windows 7 and Vista can take advantage of AVG's desktop widget, which displays protection status, and provides Scan Now and Update Now buttons:



We found the new interface design in AVG Internet Security 2013 to be exceptionally easy to navigate, with important functions and information clearly displayed and easily accessible on the home page. Our only suggestion for improvement would be to display the licence status on the home page, and move the "advertising" links in the middle row to the Options menu.

Default configuration

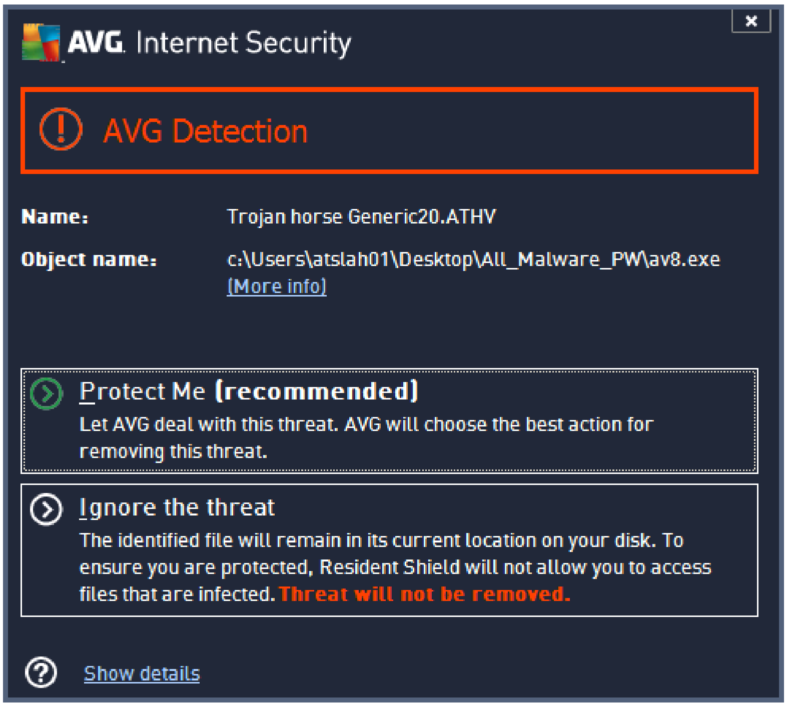
Non-administrator access

When logged on to the computer with a non-administrator Windows account, attempting to change important settings, e.g. disable real-time protection, produces a Windows UAC prompt for administrator credentials. Unless these are entered, the configuration settings remain locked. We regard this as ideal.

Scanning and malware discovery

A scheduled scan is not pre-configured, but can be set up very easily by clicking on the Scan Options button, then Manage Scheduled Scans.

When malware is discovered by the real-time protection component, there is a choice of Protect Me (which deletes or quarantines the threat) or Ignore the Threat, although this clearly states that access to the suspicious file(s) will be blocked:



AVG Detection

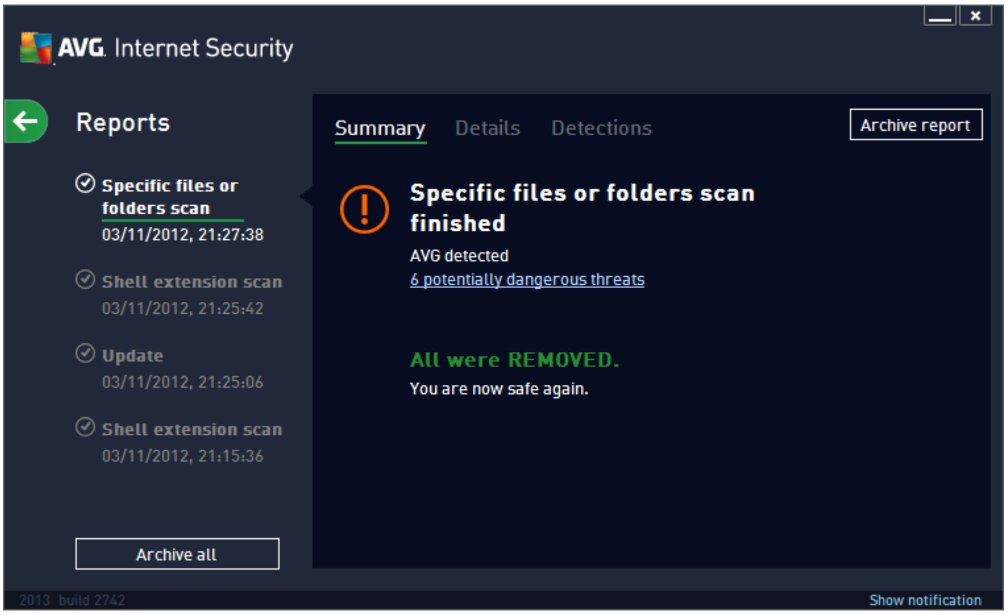
Name: Trojan horse Generic20.ATHV

Object name: c:\Users\atslah01\Desktop\All_Malware_PW\av8.exe
(More info)

Protect Me **(recommended)**
Let AVG deal with this threat. AVG will choose the best action for removing this threat.

Ignore the threat
The identified file will remain in its current location on your disk. To ensure you are protected, Resident Shield will not allow you to access files that are infected. **Threat will not be removed.**

If a scan is run from the console, malware items are simply removed:



Specific files or folders scan
03/11/2012, 21:27:38

Shell extension scan
03/11/2012, 21:25:42

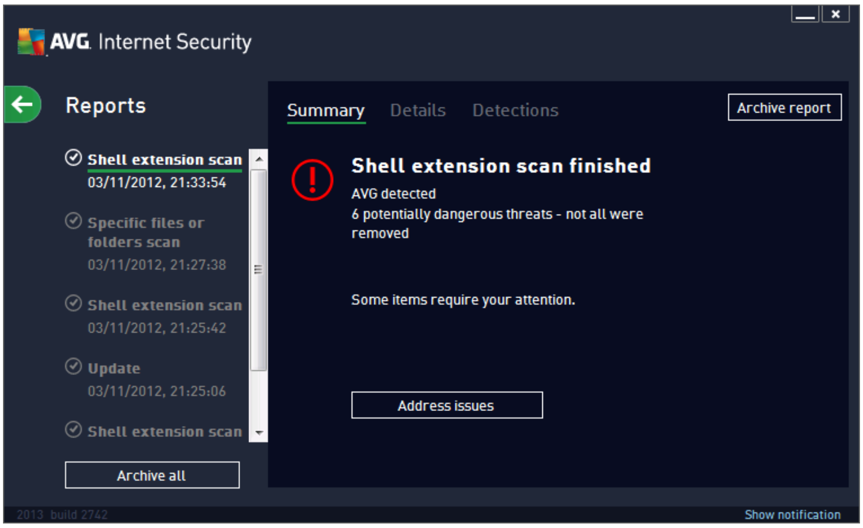
Update
03/11/2012, 21:25:06

Shell extension scan
03/11/2012, 21:15:36

Specific files or folders scan finished
AVG detected
6 potentially dangerous threats

All were REMOVED.
You are now safe again.

If a context-menu scan is run, the user is given the choice of what to do with the items discovered:



AVG Internet Security

Reports

Summary Details Detections

Archive report

Shell extension scan
03/11/2012, 21:33:54

Specific files or folders scan
03/11/2012, 21:27:38

Shell extension scan
03/11/2012, 21:25:42

Update
03/11/2012, 21:25:06

Shell extension scan

Archive all

Shell extension scan finished

AVG detected
6 potentially dangerous threats - not all were removed

Some items require your attention.

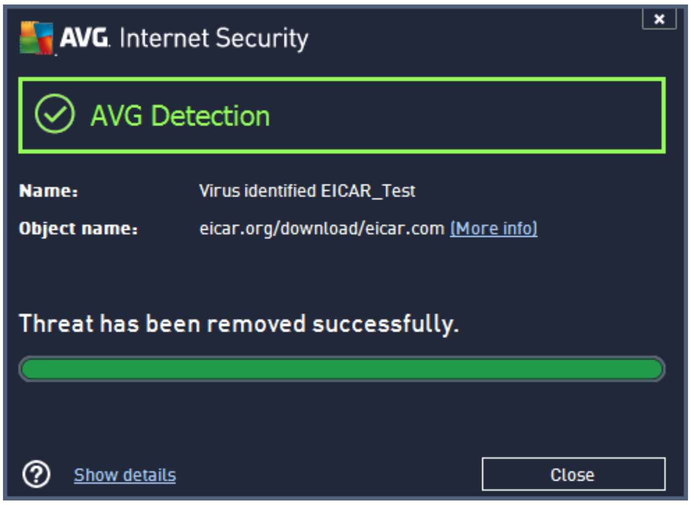
Address issues

2013 build 2742

Show notification

Clicking on Address Issues allows individual items (or all) to be selected and removed.

When we attempted to download the EICAR test file from the Internet, the file was simply deleted without question:



AVG Internet Security

AVG Detection

Name: Virus identified EICAR_Test

Object name: eicar.org/download/eicar.com (More info)

Threat has been removed successfully.

Show details

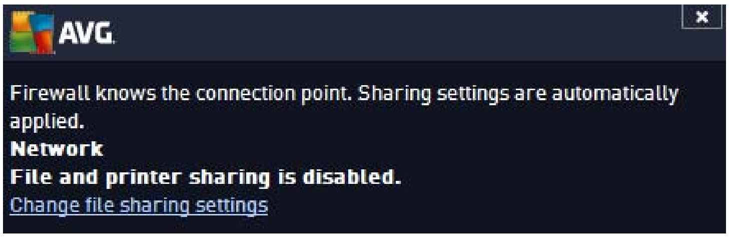
Close

We were slightly puzzled as to why some methods of malware discovery provide options for cleaning, and others do not. However, in all cases the dialog/message boxes make perfectly clear whether the user needs to take further action or not, and none of the options available would allow a malicious program to be executed.

Inbound firewall settings

As noted above, AVG's setup wizard detected the existing settings for Windows Firewall and correctly applied these to the suite's firewall. When the installation process was complete, we were still able to ping our test PC, access the file share, and connect to the machine using Remote Desktop.

Changing the network type from private to public in Windows' Network and Sharing Center prompted AVG Internet Security to show the following pop-up message:



Firewall knows the connection point. Sharing settings are automatically applied.

Network

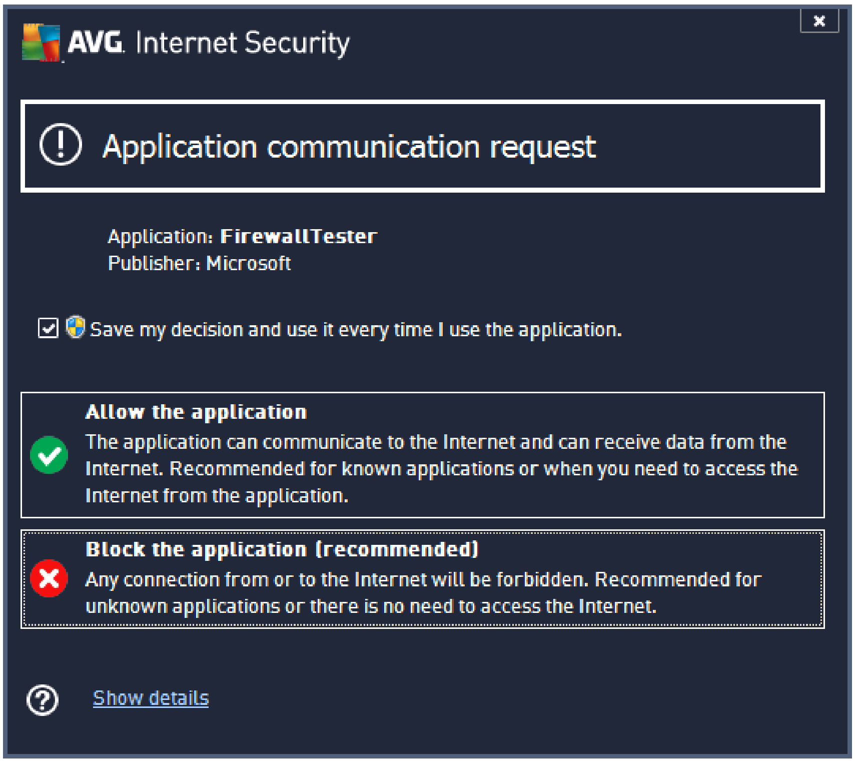
File and printer sharing is disabled.

Change file sharing settings

The suite's firewall then blocked ping, file-sharing and Remote Desktop access, although we had not changed any of AVG's own settings. We would regard this co-ordination with Windows' network settings as optimal, and find the pop-up messages reassuring.

Outbound firewall/application control

When we ran our firewall tester under default firewall settings, AVG Internet Security allowed the program to complete its test without any sort of query, which is an ideal standard configuration. Advanced users who would like more control over outgoing applications can very easily change it by setting the firewall mode to Interactive. In this mode, AVG asks whether to allow the outgoing connection:



Application communication request

Application: **FirewallTester**
Publisher: Microsoft

☑ Save my decision and use it every time I use the application.

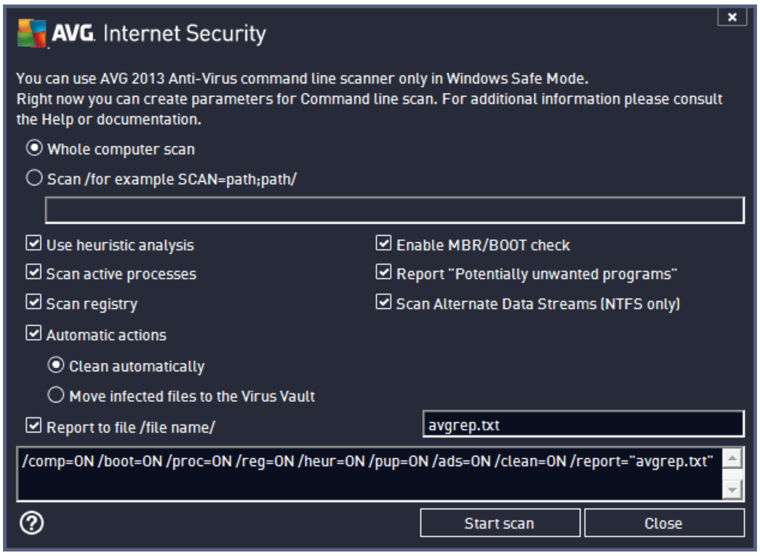
Allow the application
The application can communicate to the Internet and can receive data from the Internet. Recommended for known applications or when you need to access the Internet from the application.

Block the application (recommended)
Any connection from or to the Internet will be forbidden. Recommended for unknown applications or there is no need to access the Internet.

Show details

Safe Mode

When we started our test PC in Safe Mode with Networking, we found that AVG's real-time protection was not running, and the "Scan with AVG" item on the Explorer context menu was inoperative. However, clicking on the suite's icon in the Start Menu opens the following Safe Mode dialog box:



You can use AVG 2013 Anti-Virus command line scanner only in Windows Safe Mode.
Right now you can create parameters for Command line scan. For additional information please consult the Help or documentation.

● Whole computer scan
○ Scan /for example SCAN=path;path/

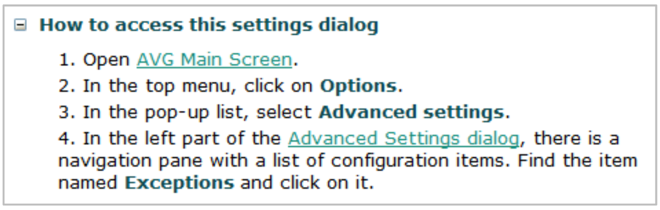
☑ Use heuristic analysis
☑ Scan active processes
☑ Scan registry
☑ Automatic actions
● Clean automatically
○ Move infected files to the Virus Vault
☑ Enable MBR/BOOT check
☑ Report "Potentially unwanted programs"
☑ Scan Alternate Data Streams (NTFS only)
☑ Report to file /file name/ avgrep.txt

```
/comp=ON /boot=ON /proc=ON /reg=ON /heur=ON /pup=ON /ads=ON /clean=ON /report="avgrep.txt"
```

This does not have an update function, but allows full or custom scans to be carried out, with various options. We ran a custom scan of our folder of malware samples, and it removed all the malware silently.

Help and documentation

The local help function is accessed from the Options menu in the top right-hand corner of the window (not Support, as one might have expected). We very quickly found answers to both our queries, i.e. how to set a scheduled scan and how to configure scan exceptions. The instructions were clear and simple in both cases, and we particularly liked a minimised section of the page entitled "How to access this settings dialog". This can be expanded to show further instructions for navigating to the relevant dialog box:



⊟ **How to access this settings dialog**

1. Open AVG Main Screen.
2. In the top menu, click on **Options**.
3. In the pop-up list, select **Advanced settings**.
4. In the left part of the Advanced Settings dialog, there is a navigation pane with a list of configuration items. Find the item named **Exceptions** and click on it.

The help functions on AVG's website can be accessed by clicking on Get Support on the Options menu. This opens the main support page in the computer's default browser; a search function can be found by clicking on FAQ and then Technical FAQ. Again, we almost instantly found concise and comprehensible instructions for both tasks.

A comprehensive, 145-page user manual can be downloaded in PDF format from the AVG website; it is very easily found in the Support menu on the home page of the site. The manual is has been produced to an excellent standard; it is clearly written, well organised and indexed, fully bookmarked, and contains abundant screenshots.

Our overall impression is that AVG's help functions and documentation can be regarded as exemplary.

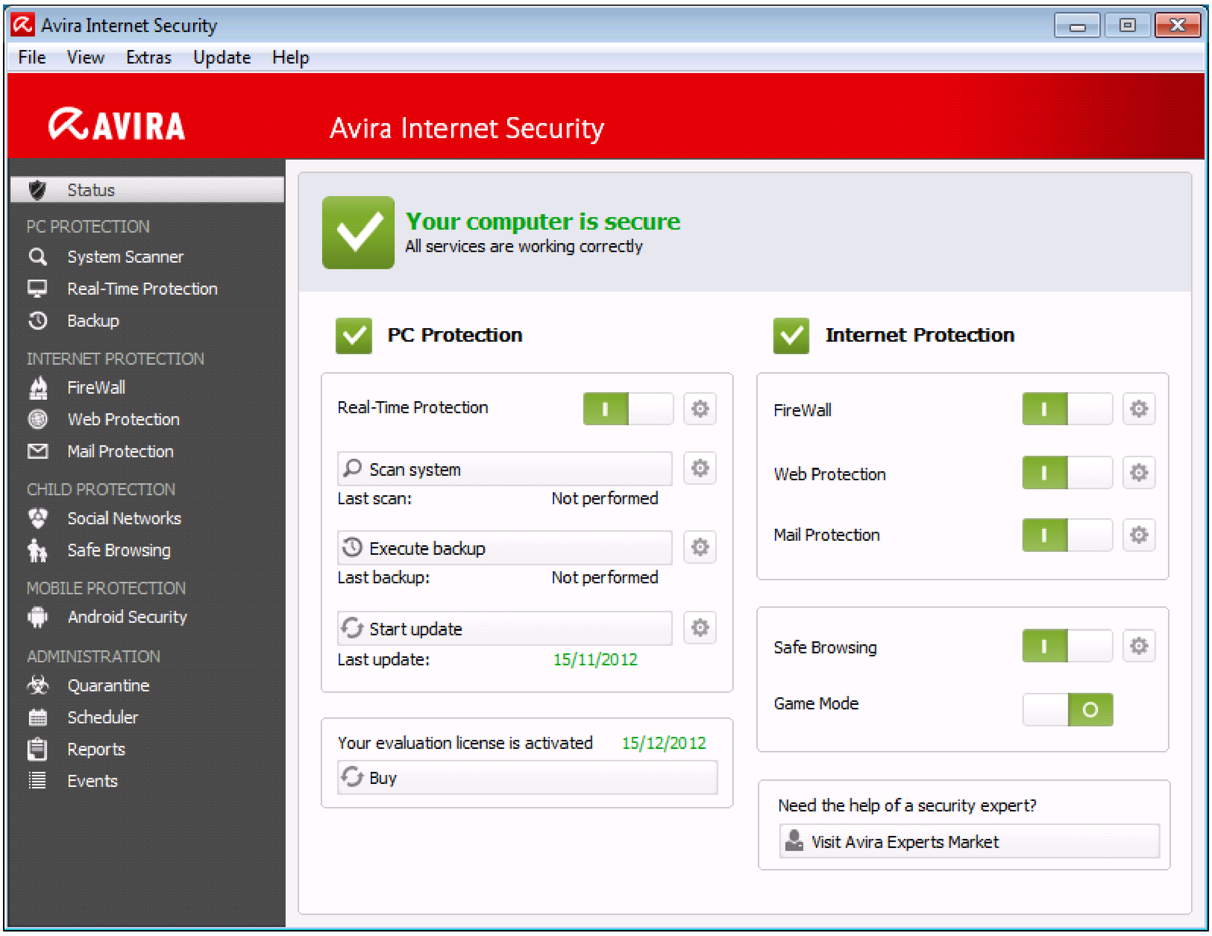
Verdict

Despite completely overhauling the interface of their Internet Security Suite, AVG have in our opinion retained all of the user-friendliness of older versions in the 2013 release. We found it exceptionally easy to use, whilst allowing advanced users a range of configuration options. The designers have obviously paid attention to detail, and we would suggest that it would be very hard to improve on for ease of use.

We were particularly impressed with the options available for advanced users in the setup/uninstall wizards; the simple but effective layout of the program window; ideal default settings; clear information and warning messages; accessible, effective and comprehensible help functions and documentation.

A minor suggestion for improvement would be enabling the update of virus signatures when used in Safe Mode with Networking.

Avira Internet Security 2013



Your computer is secure
All services are working correctly

Real-Time Protection I

Last scan: Not performed

Last backup: Not performed

Last update: 15/11/2012

Your evaluation license is activated 15/12/2012

FireWall I

Web Protection I

Mail Protection I

Safe Browsing I

Game Mode O

Need the help of a security expert?

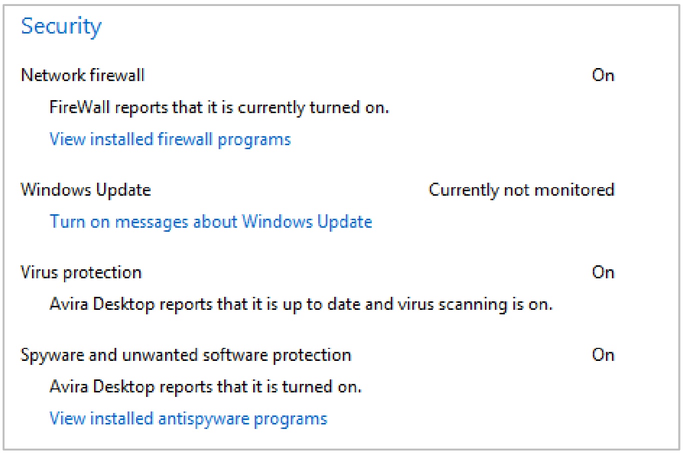
Components

Avira Internet Security 2013 comprises an antimalware component with email scanning, antispam, and a firewall. There are also parental control and backup features.

Installation

We installed the trial version of Avira Internet Security, which is supplied as a 2 MB downloader file. The setup wizard provides a one-time choice of common European and Asian languages, and allows the user to opt in or out of malware data sharing. There are Express and Custom Install options, we chose the latter. This provided us with a complete choice of components to install, the option of using the Avira search service and toolbar, a choice of the level of heuristics to be used, and the Safe Start option, which loads the antimalware component early in the boot process. The wizard also asks whether file sharing should be enabled; we accepted the default “Yes”. We were prompted to restart the computer when the wizard had finished.

Avira Internet Security 2013 registers itself with Windows Action Center as an antivirus and antispyware program and firewall:



Security

Network firewall — On

FireWall reports that it is currently turned on.

View installed firewall programs

Windows Update — Currently not monitored

Turn on messages about Windows Update

Virus protection — On

Avira Desktop reports that it is up to date and virus scanning is on.

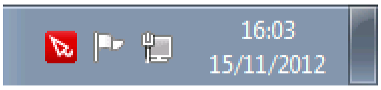
Spyware and unwanted software protection — On

Avira Desktop reports that it is turned on.

View installed antispyware programs

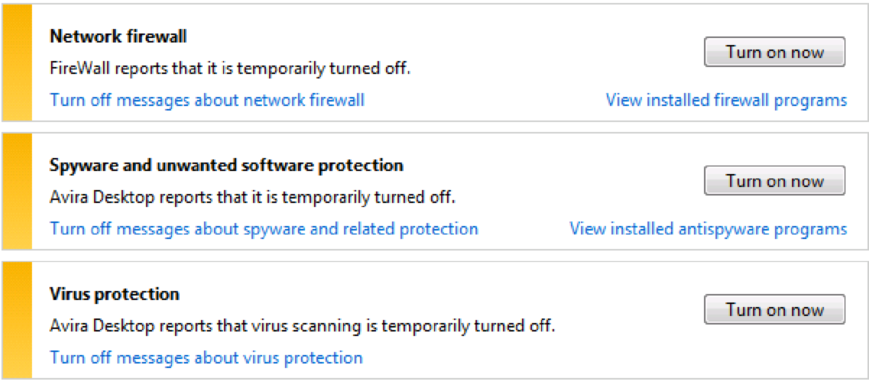
We are not sure why the firewall component does not show the Avira name; this would appear to be a missed advertising opportunity for Avira, and may leave some users wondering who the maker of their firewall is. Both Windows Firewall and Windows Defender are disabled.

When Avira's firewall or real-time protection components are disabled, Windows Action Center does display a warning, but this is much less obvious than the standard warning we would expect. There is no warning message or changed Action Center icon visible in the system tray (although the Avira icon itself does change, from an open umbrella to a closed one):



Avira System Tray icons

Additionally, the warning message in the Action Center window is yellow rather than red, and reports that Avira is "temporarily" turned off:



Network firewall

FireWall reports that it is temporarily turned off.

Turn off messages about network firewall

Turn on now
View installed firewall programs

Spyware and unwanted software protection

Avira Desktop reports that it is temporarily turned off.

Turn off messages about spyware and related protection

Turn on now
View installed antispyware programs

Virus protection

Avira Desktop reports that virus scanning is temporarily turned off.

Turn off messages about virus protection

Avira Action Center Warning

We feel that the muted warning from Windows Action Center is much less obvious than the standard warning message, and would not be apparent to users unless they deliberately checked the Action

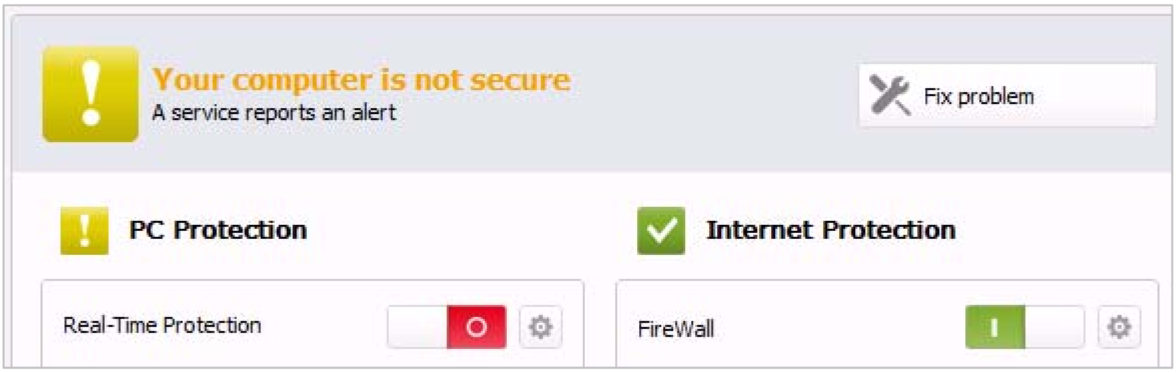
Center. We would urge Avira to reconsider the suite's interaction with Action Center and implement the standard warning when important protection components are turned off.

Avira's uninstaller provides two options, Remove and Change. The latter allows selective removal of components, so that e.g. the firewall (or any other individual component) could be removed, but leave the remainder of the suite.

Avira tell us that running the Change option will perform a *de facto* repair installation. However, there is nothing in the uninstaller program to inform the user of this, so most users would assume that there is no repair option.

Program interface

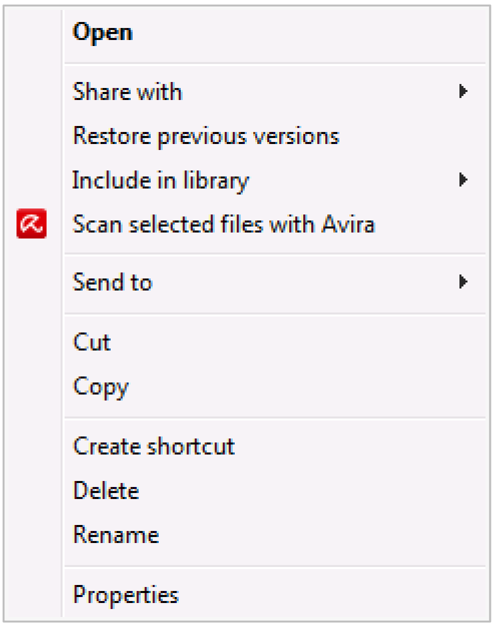
The main program window of Avira Internet Security 2013 retains its familiar layout, with a narrow left-hand menu column and a much larger main pane on the right to display the details selected on the left. There have been some minor changes since the 2012 edition, but the overall design remains unchanged. There is a prominent status display at the top, with a tick (checkmark) in a green box, and the wording "Your computer is secure", if all is well. This changes to an exclamation mark on yellow, and the text "Your computer is not secure", if an important component is disabled. A button marked "Fix problem" appears, and the on/off switch for the item concerned turns red; either can be used to reactivate the component.



Your computer is not secure
A service reports an alert

The Status (home) page of the window also includes buttons to launch an update and a full system scan, and the licence expiry date is also displayed. Help functions can be accessed from the Help menu in the traditional menu bar at the top of the window.

Avira Internet Security adds a scan entry on Windows Explorer's context menu:



Default configuration

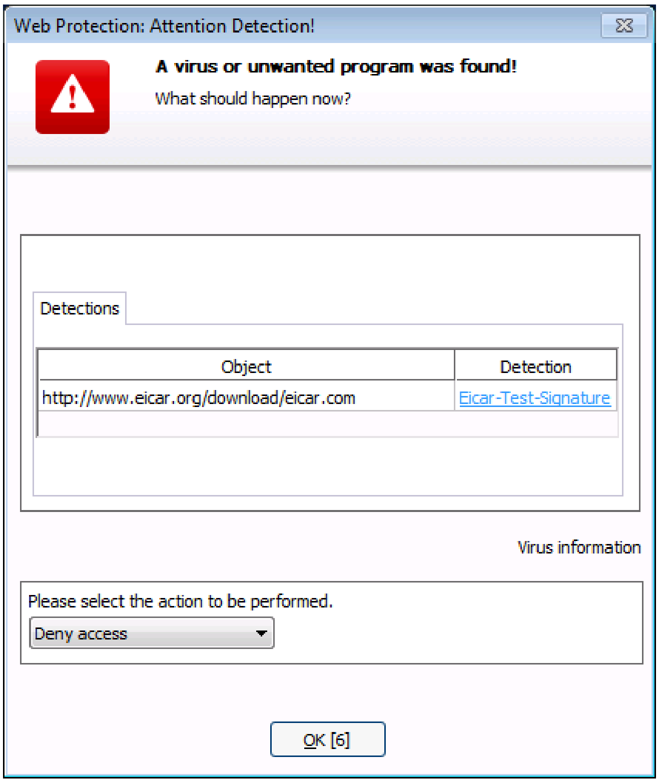
Non-administrator access

When we logged on to our test PC with a non-administrator account, we were still able to disable the firewall and real-time protection without any sort of restriction or challenge. We feel this is not ideal for a suite which is obviously aimed at family use. It is possible to password protect the settings for all users, though we feel that the setup wizard should prompt users to set this during installation.

Scanning and malware discovery

A Quick System Scan is scheduled to run every 168 hours. This can be changed, or new scheduled scans set, from the Scheduler item in the menu panel on the left. We could not find a means of running a boot-time scan, although setup does provide an option to load the antivirus protection early in the boot process.

When we attempted to download the EICAR test file, Avira Internet Security blocked the download and the web page, and displayed the following dialog box:



Web Protection: Attention Detection!

A virus or unwanted program was found!

What should happen now?

Detections

Object	Detection
http://www.eicar.org/download/eicar.com	Eicar-Test-Signature

Virus information

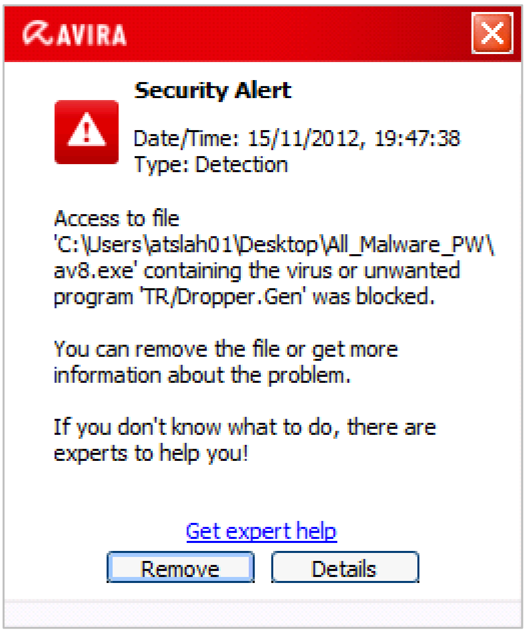
Please select the action to be performed.

Deny access

OK [6]

The default action (deny access) is taken unless the user chooses another action within 10 seconds. Whilst this protects the computer effectively, we feel the dialog box may be a little confusing to non-experts.

When malware was discovered locally by Avira's real-time protection, this dialog box was shown:



AVIRA

Security Alert

Date/Time: 15/11/2012, 19:47:38
Type: Detection

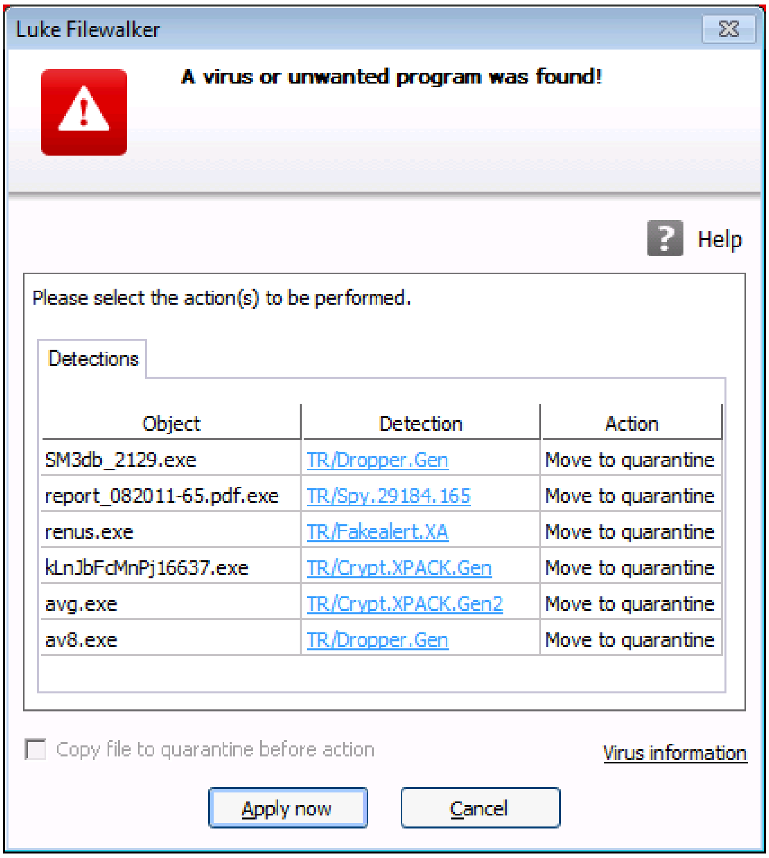
Access to file 'C:\Users\atslah01\Desktop\All_Malware_PW\av8.exe' containing the virus or unwanted program 'TR/Dropper.Gen' was blocked.

You can remove the file or get more information about the problem.

If you don't know what to do, there are experts to help you!

The user has the choice of Remove or Details; the latter runs a quick scan, then displays a dialog box showing the malware found and the option to quarantine it. The malware will not run, even if the user does not choose the Remove or Quarantine options.

Running a scan from the console or context menu displays the malware items found, and allows the user to quarantine them with a single click:



A virus or unwanted program was found!

Please select the action(s) to be performed.

Object	Detection	Action
SM3db_2129.exe	TR/Dropper.Gen	Move to quarantine
report_082011-65.pdf.exe	TR/Spy.29184.165	Move to quarantine
renus.exe	TR/Fakealert.XA	Move to quarantine
kLnJbFcMnPj16637.exe	TR/Crypt.XPACK.Gen	Move to quarantine
avg.exe	TR/Crypt.XPACK.Gen2	Move to quarantine
av8.exe	TR/Dropper.Gen	Move to quarantine

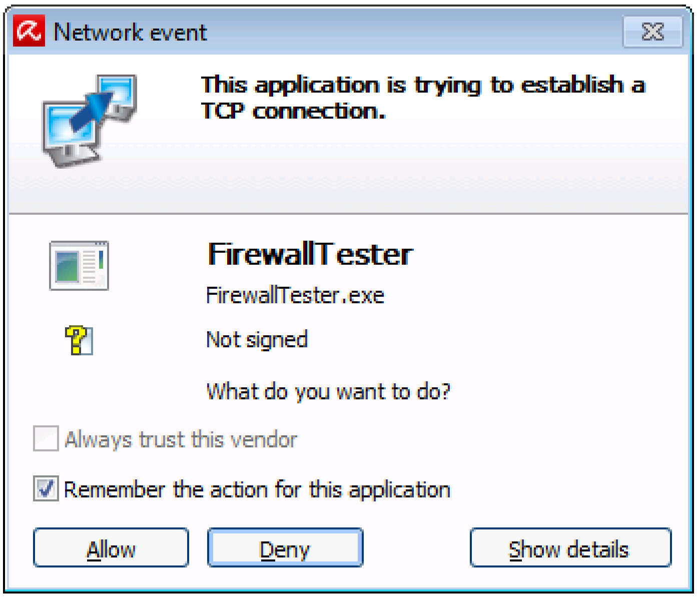
□ Copy file to quarantine before action

Inbound firewall settings

After installing Avira Internet Security 2013, we were still able to access our test PC's file share, ping it, and control it by Remote Desktop, just as before we installed the suite. We note that Avira's setup wizard asked us whether to allow file sharing, but did not prompt us to define the current network type as public or private. Changing the network type from Work to Public in Windows' Network and Sharing Center had no effect on access to the PC over the network. We also found that connecting to a new network, which we defined as Public when prompted by Windows, still made no change to the firewall settings in Avira Internet Security, which continued to allow pinging, file share and Remote Desktop access. To block access to our test PC from the network, we had to change the security level from the default Medium setting to High in Avira's Firewall settings. There isno co-ordination between the network type set in Windows' Network and Sharing Center and the functioning of the Avira firewall. Avira's security policy is based on changing the firewall settings, rather than defining a network type in the way that Windows does. We are concerned that this could lead to users believing they were protected on public networks, because they had selected Public in Network and Sharing Center, whilst the Avira firewall settings were still allowing access.

Outbound firewall/application control

When we ran our firewall testing program, Avira Internet Security 2013 displayed the following dialog box, asking whether the program should be allowed to access the Internet:



Network event

This application is trying to establish a TCP connection.

FirewallTester

FirewallTester.exe

Not signed

What do you want to do?

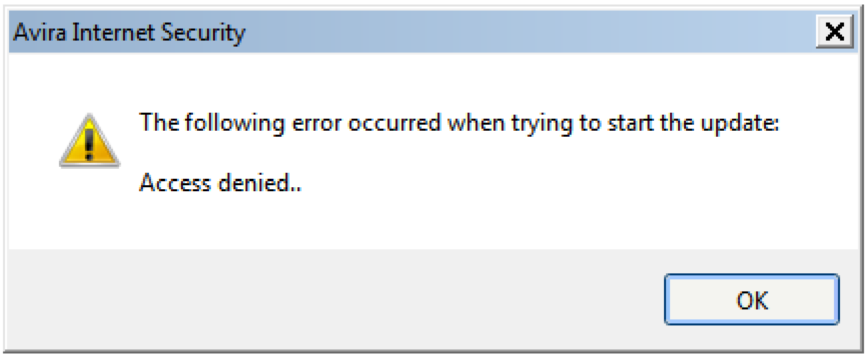
□ Always trust this vendor

☑ Remember the action for this application

We feel that this is not an ideal default setting for non-expert users, who will probably have no idea which processes should be allowed and which not. We were unable to find an obvious means of completely disabling prompts for outgoing processes, only of allowing individual programs Internet access.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were able to run a context-menu scan of our malware folder, which removed all the items, exactly as it would in normal mode. When we attempted to run a signature update, the following message was displayed:



Avira Internet Security

The following error occurred when trying to start the update:

Access denied..

We therefore assume that the update failed.

Help and documentation

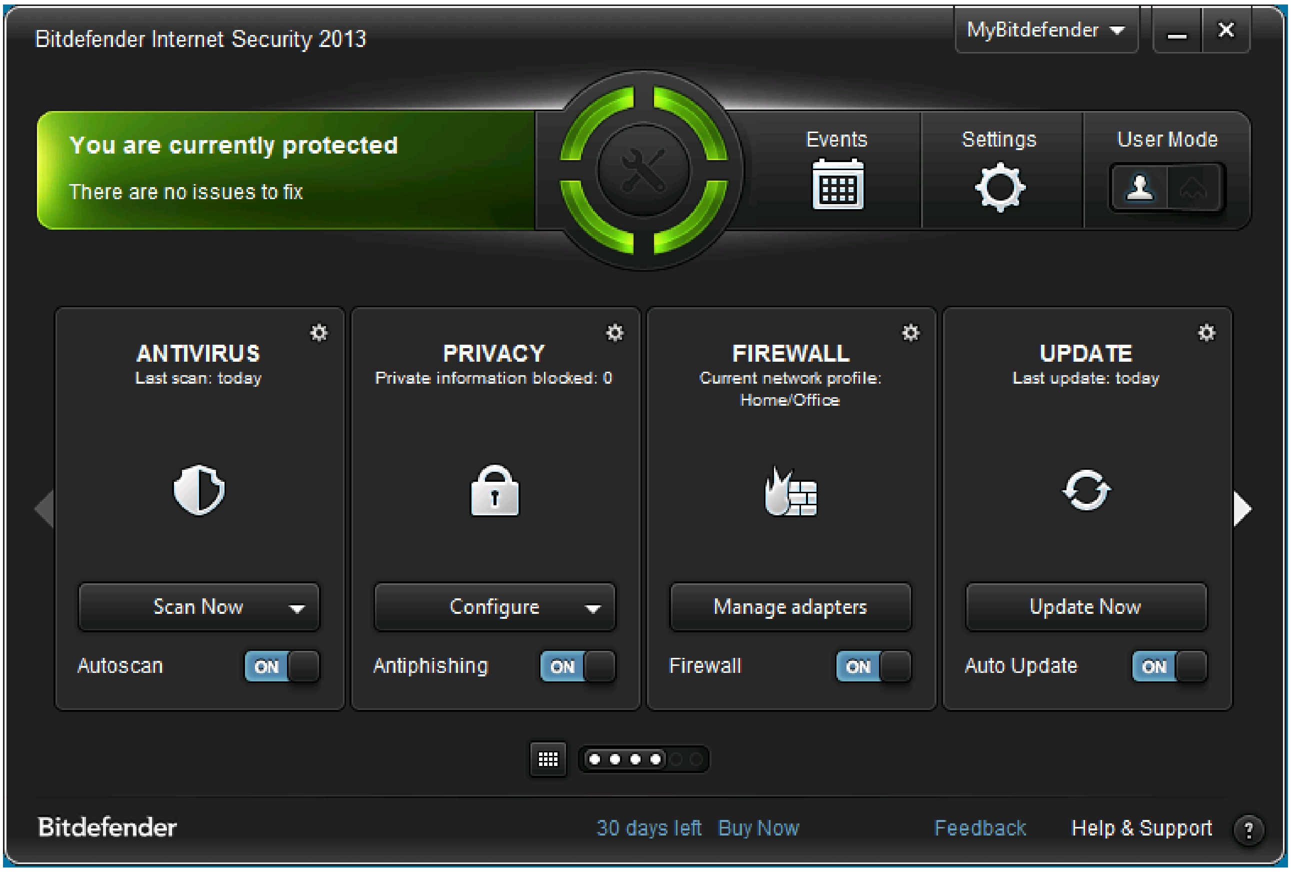
Avira Internet Security 2013 has a local help function. We quickly managed to find entries relating to scheduling a scan and setting scan exceptions. However, we felt that they would not adequately describe to a non-expert user how to find the functions concerned, only how to use them once they have been located.

The manual can easily be downloaded from the Help menu, which we found very convenient. It is very comprehensive at 233 pages. The document has been very professionally produced, has an extensive table of contents with links to the pages concerned, and has been well bookmarked. It is thus very easy to find a particular page or section very quickly. We found the instructions for setting scan exceptions and scheduling to be more user-friendly than in the local help service. There is also an online knowledge base, which appears to be oriented towards advanced users.

Verdict

We found the program window layout of Avira Internet Security 2013 to be clear and modern, providing easy access to all important features and information. The manual is comprehensive, very well produced, and easy to find. However, we have some concerns about the firewall, which appears not to reconfigure itself automatically for public networks, or prompt users that they need to do this. We would urge Avira to rectify this. We also feel that a suite obviously intended for family use should prevent non-administrator accounts from disabling essential components.

Bitdefender Internet Security 2013



Bitdefender Internet Security 2013

You are currently protected

There are no issues to fix

ANTIVIRUS
Last scan: today
Autoscan ON

PRIVACY
Private information blocked: 0
Antiphishing ON

FIREWALL
Current network profile: Home/Office
Firewall ON

UPDATE
Last update: today
Auto Update ON

30 days left

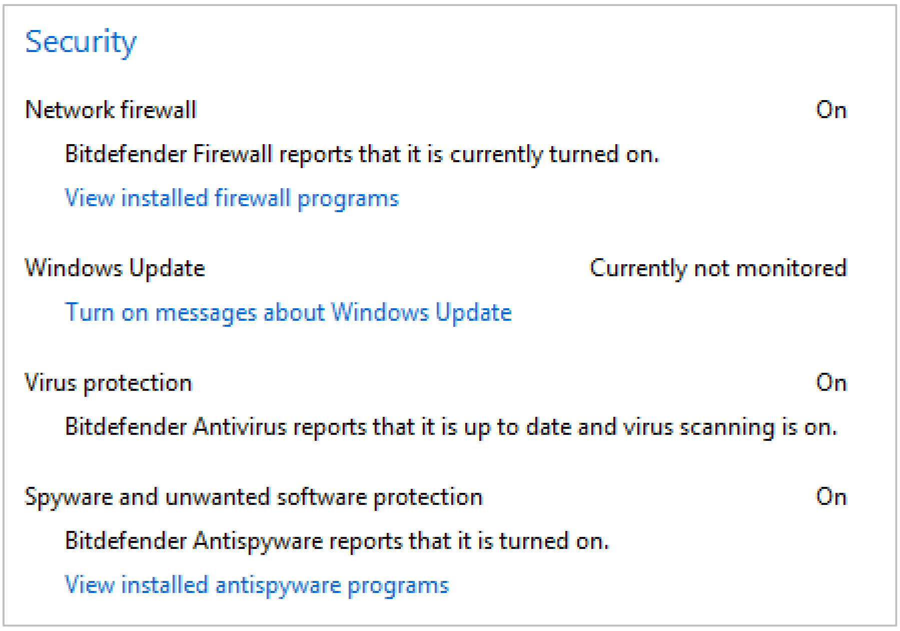
Components

Bitdefender Internet Security 2013 includes an antimalware component with email scanning, antispam, and a firewall. It also includes a secure deletion function.

Installation

We installed the trial version of Bitdefender Internet Security, which is supplied as a 2.3 MB downloader file. The first page of the setup wizard requires accepting the licence agreement, deciding whether to send usage reports to the manufacturer, and opting for a standard or customised installation. We chose the latter. Further steps included choosing the installation folder location, entering a licence key or using the trial, and opting in our out of Autopilot and Automatic Game mode. There is no choice of components to be installed. The wizard does allow "configuration" of components, allowing e.g. the antispam and firewall components to be deactivated, but the same could be done later from the console. A reboot was not required.

Bitdefender Internet Security registers itself in Windows Action Center as an antivirus and antispyware program and firewall. Both Windows Firewall and Windows Defender are disabled. If the suite's real-time protection or firewall is turned off, Action Center immediately displays its normal alerts.



Security

Network firewall On

Bitdefender Firewall reports that it is currently turned on.

View installed firewall programs

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

Bitdefender Antivirus reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

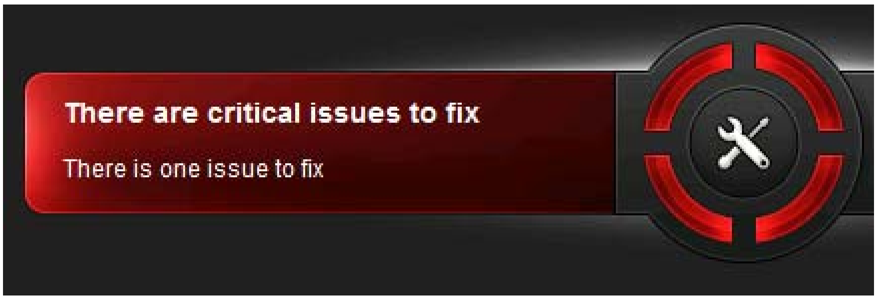
Bitdefender Antispyware reports that it is turned on.

View installed antispyware programs

Bitdefender's uninstaller includes a repair option as well as complete removal of the suite.

Program interface

The layout of the Bitdefender Internet Security 2013 window is very similar to the 2012 version, with only minor changes having been made. There is an obvious status display at the top of the window, which states "You are currently protected" on a green background if all is well. If an important component is disabled, the text changes to "There are critical issues to fix" on red:



There are critical issues to fix

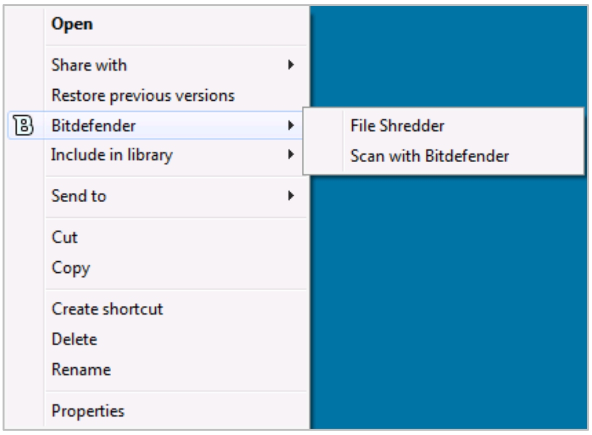
There is one issue to fix

The entire status display area turns into a "Fix All" button, i.e. clicking anywhere on it opens a page that allows the disabled component to be reactivated easily.

The main part of the window consists of four panels, displaying Antivirus, Privacy, Firewall, and Update (by default). An arrow on the right-hand side allows the user to scroll through additional functions, such as Antispam.

The Antivirus panel contains a Scan Now button, which presents a menu of scan options, including Quick Scan, System Scan and Custom Scan.

Bitdefender adds its own sub-menu to the Windows Explorer context menu, with the entries File Shredder and Scan with Bitdefender:



The Help function and subscription information can be found at the bottom of the window.

Default configuration

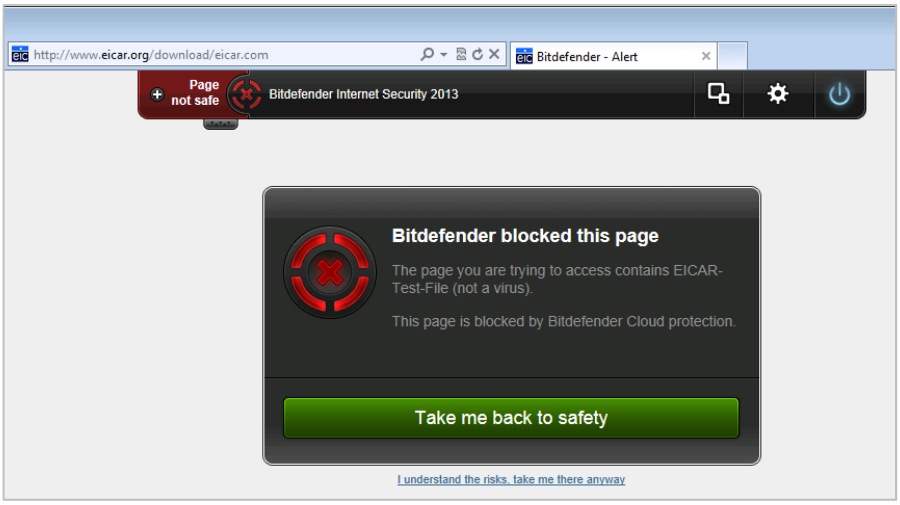
Non-administrator access

When we logged on to our test PC with a non-administrator account, we found that we could not disable the real-time protection or firewall, which we consider to be ideal.

Scanning and malware discovery

Bitdefender Internet Security 2013 does not have a scheduler function, but we understand that it runs idle-time scans, i.e. an automatic scan whenever the computer is not being used. We could not find any way of running a boot-time scan, although we note that a vulnerability scan is offered.

When we tried to download the EICAR test file, Bitdefender blocked the webpage with the following warning:

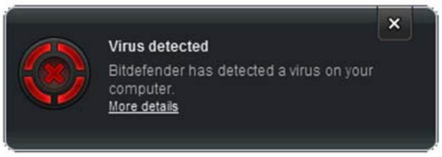

http://www.eicar.org/download/eicar.com
Bitdefender - Alert
Page not safe
Bitdefender Internet Security 2013
Take me back to safety
I understand the risks, take me there anyway

Bitdefender blocked this page

The page you are trying to access contains EICAR-Test-File (not a virus).

This page is blocked by Bitdefender Cloud protection.

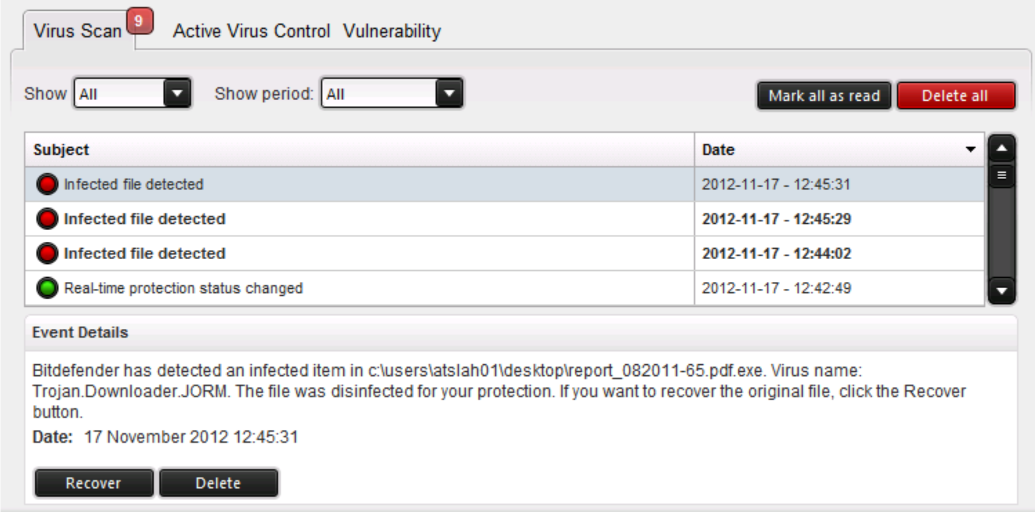
When we clicked on "I understand the risks, take me there anyway", Bitdefender blocked the file download and displayed the following alert:



Virus detected

Bitdefender has detected a virus on your computer.

We note that this only states that a virus has been detected, not that it has been deleted or quarantined, which may leave some users worried about whether they have been infected or need to take any action. Clicking on "More details" does however show that the file has been deleted:



Show: All   Show period: All

Subject	Date
🟥 Infected file detected	2012-11-17 - 12:45:31
🟥 **Infected file detected**	**2012-11-17 - 12:45:29**
🟥 **Infected file detected**	**2012-11-17 - 12:44:02**
🟩 Real-time protection status changed	2012-11-17 - 12:42:49

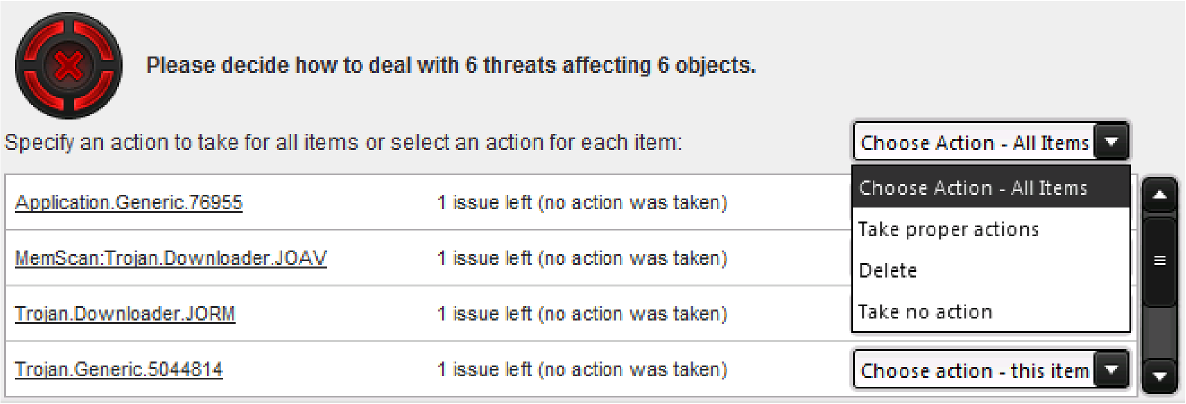
Event Details

Bitdefender has detected an infected item in c:\users\atslah01\desktop\report_082011-65.pdf.exe. Virus name: Trojan.Downloader.JORM. The file was disinfected for your protection. If you want to recover the original file, click the Recover button.

Date: 17 November 2012 12:45:31

Bitdefender reacted to local malware discovered by the real-time protection in the same way as to the EICAR file.

When we ran a custom or context-menu scan on our malware folder, Bitdefender Internet Security displayed the following list of items, with a choice of actions for each individual item or one action for all items (in the screenshot below, the Choose Action – All Items menu is shown):



Please decide how to deal with 6 threats affecting 6 objects.

Specify an action to take for all items or select an action for each item:

Application.Generic.76955	1 issue left (no action was taken)
MemScan:Trojan.Downloader.JOAV	1 issue left (no action was taken)
Trojan.Downloader.JORM	1 issue left (no action was taken)
Trojan.Generic.5044814	1 issue left (no action was taken)

Choose Action - All Items
Choose Action - All Items
Take proper actions
Delete
Take no action
Choose action - this item

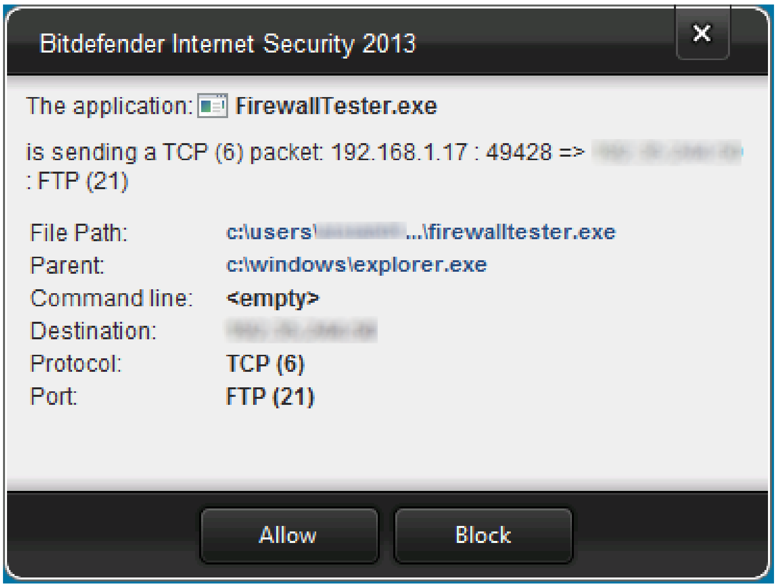
We find the term “Take proper actions” rather strange, as it might suggest anything else would be an improper action. We suggest “Take recommended action” would be clearer. However, we selected this action anyway, and all the malware items found were deleted.

Inbound firewall settings

After installing Bitdefender Internet Security 2013, we were able to ping our test PC, access its file share, and control it by Remote Desktop, just as before. Changing the network type from Work to Public in Windows’ Network and Sharing Center has no effect on Bitdefender’s firewall settings. When we manually changed the Bitdefender firewall to public, we found that pinging and file share access were blocked, but that Remote Desktop access remained unchanged. When we changed to a different network, which we designated as Public in Windows Network and Sharing Center, Bitdefender’s firewall also registered the network as Public. We found that pinging and file sharing were completely blocked, as was Remote Desktop access using the test PC’s hostname. However, we were still able to log on to the test PC with Remote Desktop if we used its IP address (v6). We would suggest that this is a significant flaw, and would urge Bitdefender to investigate it.

Outbound firewall/application control

When we ran our firewall testing program, Bitdefender allowed it to complete its task without any sort of alert. Enabling the firewall's Paranoid Mode (not an ideal description, we feel) produced the following prompt when the firewall tester was run again:



Bitdefender Internet Security 2013

The application: FirewallTester.exe

is sending a TCP (6) packet: 192.168.1.17 : 49428 => [redacted] : FTP (21)

File Path:	c:\users\[redacted]...\firewalltester.exe
Parent:	c:\windows\explorer.exe
Command line:	<empty>
Destination:	[redacted]
Protocol:	TCP (6)
Port:	FTP (21)

We note that once we had clicked Allow, this action was remembered, and the prompt did not appear again for this program.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were unable to open the Bitdefender Internet Security interface or start an update. However, we were able to run a context-menu scan of our malware folder, which ran and removed all items just as it would in normal mode.

Help and documentation

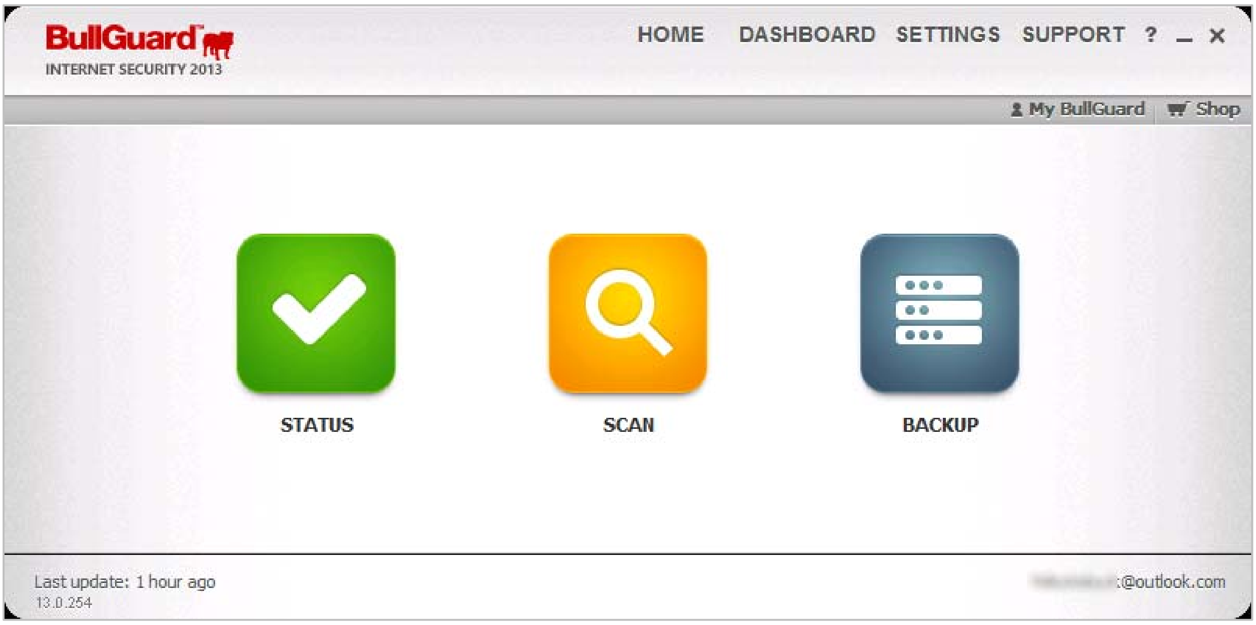
Bitdefender Internet Security 2013 has local and online Help functions, both of which are accessible from the program's Help window. We quickly found clear and simple instructions for setting scan exclusions in both Help features; we noted that the answers were extremely similar to each other.

Bitdefender produce a comprehensive, 171-page manual for Internet Security 2013, which we found easily on the website. It has been very well produced, with an extremely detailed table of contents with links to each page/section, and extensive bookmarking, making it very easy to find an item very quickly and easily. The manual has been well written and clearly formatted, but is unfortunately almost entirely lacking in screenshots, with only pictures of individual icons for illustration.

Verdict

By and large, Bitdefender Internet Security 2013 is well designed, with important functions and information easily accessible. There is a comprehensive, well-produced manual to go with it. We found some of Bitdefender's terminology rather confusing, however. We are also concerned that we were able to access our test PC using a Remote Desktop connection, even though the suite's firewall was set to Public mode.

BullGuard Internet Security 2013

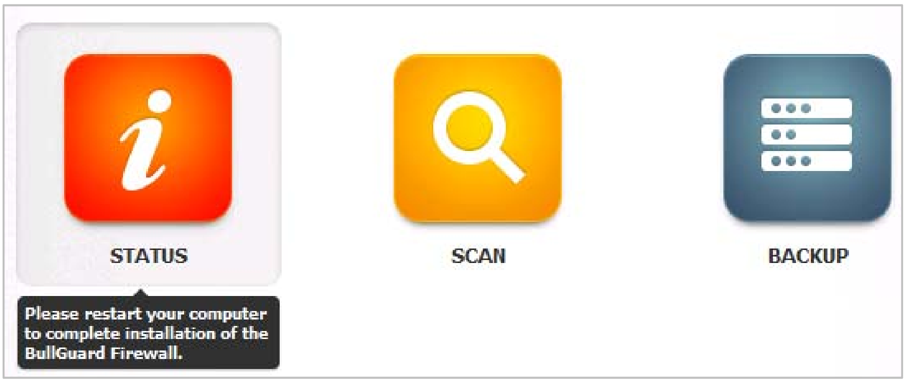


Components

BullGuard Internet Security 2013 includes an antimalware component with email scanning, antispam, a firewall, parental controls, and a backup function.

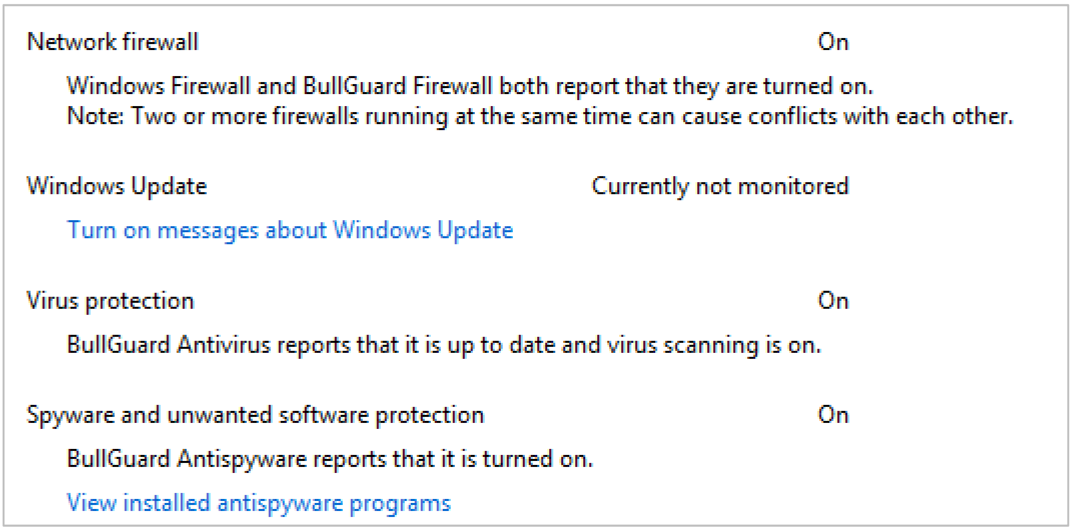
Installation

We installed BullGuard Internet Security using the 365 KB downloader file provided for the trial version. This saves a 25 MB full installer file on the current user's desktop. Installation involves accepting a licence agreement, then deciding whether to use the Custom or standard installation (we chose the former). The only options this provided were the location of the installation folder, and whether or not to disable Windows Defender. We chose the default "yes" here. A reboot is recommend at the end of the installation process, but this only becomes apparent if the user opens the main program window and moves the mouse over the status icon:



Please restart your computer to complete installation of the BullGuard Firewall.

BullGuard Internet Security 2013 registers with Windows Action Center as an antivirus and antispyware program and firewall. Windows Defender is disabled by default, but Windows Firewall is not:



Network firewall On

Windows Firewall and BullGuard Firewall both report that they are turned on.
Note: Two or more firewalls running at the same time can cause conflicts with each other.

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

BullGuard Antivirus reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

BullGuard Antispyware reports that it is turned on.

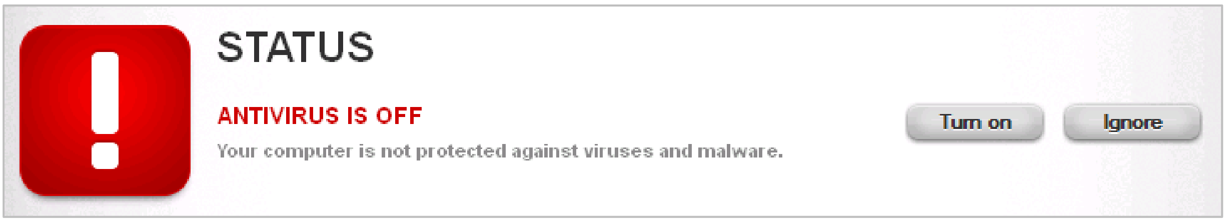
View installed antispyware programs

We are surprised to see that the suite allows Windows Firewall to run alongside its own, given that it is generally accepted that only one software firewall should be used at a time (as noted by Windows Action Center). However, BullGuard tell us that the suite's firewall fully integrates with Windows Firewall, and that both can run at the same time without a negative effect on the computer. If BullGuard's real-time protection is disabled, Windows Action Center displays its normal alerts.

The suite's uninstaller has no options other than complete removal (although settings can be retained if desired).

Program interface

BullGuard Internet Security's main program window is dominated by three big buttons marked Status, Scan and Backup. The Status button displays a white tick (checkmark) on a green background if all is well; moving the mouse over it displays the message "Your computer is protected. No actions needed". In this state, clicking on the button has no effect. If real-time protection is disabled, the button changes to an exclamation mark on a red background; mousing over this displays the text "Your computer is not protected against viruses and malware". Clicking on it then opens a page that explains that "Antivirus is off" and provides two buttons, "Turn on" and "Ignore".



STATUS

ANTIVIRUS IS OFF

Your computer is not protected against viruses and malware.

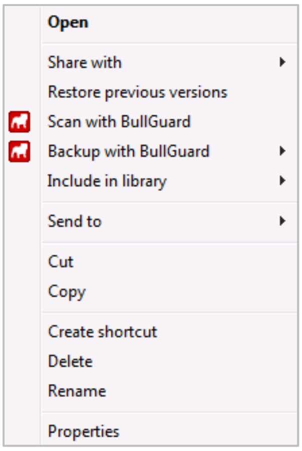
Clicking Turn On naturally reactivates the real-time protection; we were rather alarmed to see that clicking Ignore returns the Status button on the home page to its “All is well” state, text included, even though real-time protection is switched off. Even after rebooting our test PC, we found that BullGuard Internet Security was still displaying “Your computer is protected, no actions needed”, and the tick in a green box, even though Windows Action Center was clearly indicating that antivirus protection was turned off, and we were able to download the EICAR test file unimpeded.

Clicking on the Status button did not produce any further information or an option to reactivate real-time protection. We found that having clicked the Ignore button once, we could disable and reactivate the real-time protection any number of times without an alert being shown. The warning had to be manually re-enabled by using the Reset button in the General section of the program’s settings. We suggest that (accidentally) clicking the Ignore button could easily lead to users believing that their PC was protected when it wasn’t. We understand from BullGuard that they are reconsidering the inclusion/nature of the Ignore button.

The update status is displayed as small text in the bottom left-hand corner of the window, which also functions as a manual update button. Whilst this may be aesthetically very convenient, we feel many users might not realise that the text has this function, and so would look elsewhere for a means of running a manual update. However, BullGuard inform us that automatic updates run regularly, making manual update unnecessary, and that the Status screen will inform the user if the program is significantly out of date, with an obvious manual update function provided.

Clicking the Scan button on the program’s home page displays the scan options Quick Scan, Full Scan, and Tune Up (“Optimize computer performance”). Although the program does have a custom scan option, this can only be accessed by clicking on Dashboard | Antivirus, which we feel makes it rather inaccessible. We suggest that the Tune Up button is misplaced among the scan options, and that replacing it with a button for running a custom scan would make the program more intuitive. BullGuard tell us that they are considering doing this.

BullGuard Internet Security 2013 integrates itself into Windows Explorer's context menu with two entries, one for backing up files, and another for scanning for malware:



Subscription information can be found by clicking Settings | General | Account, or by clicking the My BullGuard link and logging in to the BullGuard account using the web page that this opens. We note that we did not find either method very intuitive or convenient.

The online help service can be accessed by clicking the question-mark symbol in the top right-hand corner of the window.

The menu in the window's title bar includes the items "Dashboard" and "Settings". We note that some detailed configuration options for the firewall are found under Dashboard rather than Settings, which does not seem very obvious to us.

Default configuration

Non-administrator access

When we logged on to our test PC with a non-administrator account, we were able to deactivate the real-time protection without any restriction. We do not regard this as ideal, especially in a suite which is obviously intended for family use. It is possible to password-protect important settings, but the installation wizard does not prompt the user to set this up. However, BullGuard inform us that they are reviewing this.

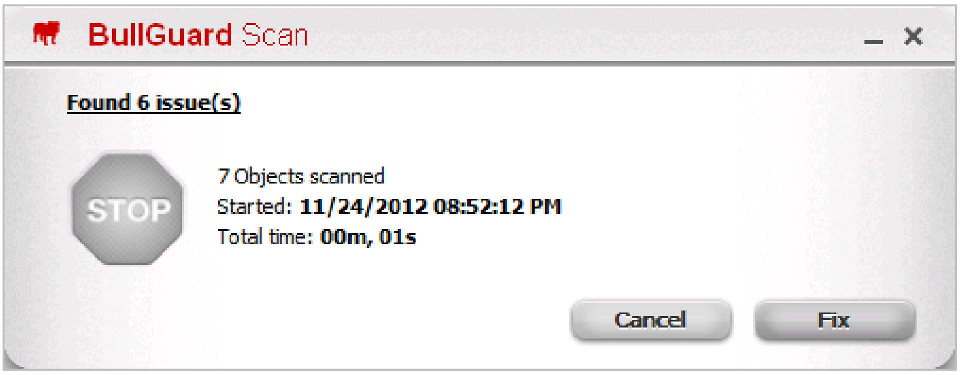
Scanning and malware discovery

A scheduled scan is not set by default. It can be configured by clicking Dashboard | Antivirus | Custom Scan, a process we did not find particularly intuitive. Clicking Quick Scan or Full Scan simply starts the scan concerned, without offering any configuration options. Clicking Custom Scan allows all existing scan profiles to be scheduled, or a new one to be created; we suggest that a separate button marked "Scheduled Scan" would be clearer.

We could not find a means of running a boot-time scan, although a rootkit scan is available.

When we attempted to download the EICAR test file, we found that it was saved in the Downloads folder but as a 0 KB file, Bullguard having silently deleted its contents. This is in accordance with the quiet mode we had selected during setup, although we feel that leaving a 0 KB file may confuse some users. When Bullguard's real-time protection discovered malware locally on the PC, it quarantined it silently.

When we ran a custom or context-menu scan on our folder of malware, BullGuard displayed the following dialog box:

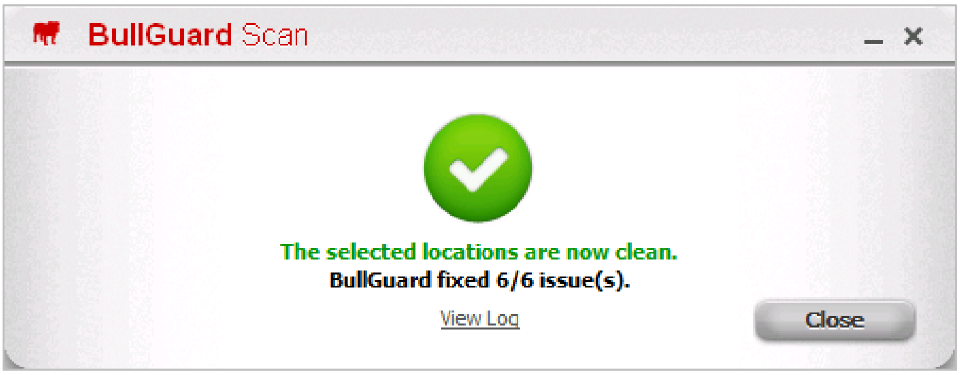


BullGuard Scan

Found 6 issue(s)

7 Objects scanned
Started: **11/24/2012 08:52:12 PM**
Total time: **00m, 01s**

Clicking Fix quarantined the malware items and informed us that it had been removed:



BullGuard Scan

The selected locations are now clean.
BullGuard fixed 6/6 issue(s).

We feel that the procedure makes it quick and easy to remove the malware found in a scan.

Inbound firewall settings

After installing BullGuard Internet Security 2013, we were able to access the file share of our test PC, and log on via Remote Desktop, just as we had before. However, we noted that we could no longer ping the machine, with either IPv4 or IPv6. A brief attempt to enable ping responses in the firewall settings failed. We understand from BullGuard that this will be corrected in the next release of the software.

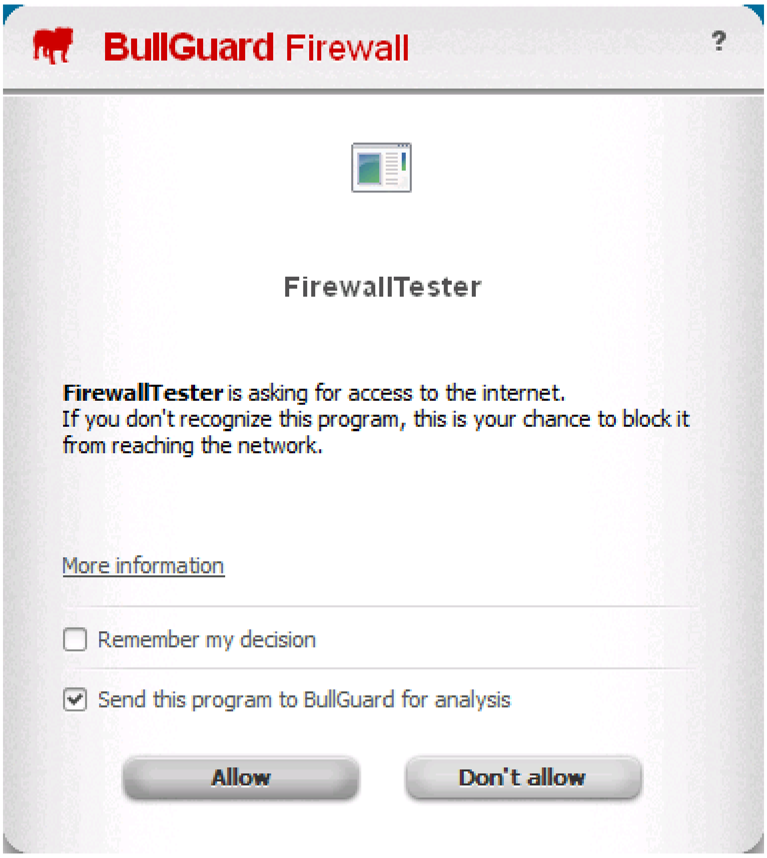
Changing the network type to Public in Windows Network and Sharing Center blocked access to the file share and prevented Remote Desktop access, regardless of whether hostname or IP address was used. Switching the network type back to Work in Windows Network and Sharing Center re-enabled file share and RDP access. We find the co-ordination between Windows and BullGuard to be ideal. We note, however, that deselecting the current subnet from the list of trusted networks in

BullGuard's firewall settings had no effect on accessibility, which advanced users should be aware of. Again, BullGuard inform us that this is a known issue which will be corrected in the next version.

Given that BullGuard does not disable Windows Firewall on installation, we felt we should also try the BullGuard firewall on its own, with Windows Firewall switched off. We found that the results were identical, with file-sharing and Remote Desktop access available when the network was defined as Work in Windows Network and Sharing Center, and disabled when Public was selected.

Outbound firewall/application control

When we ran our firewall testing program, BullGuard displayed the following dialog box:



FirewallTester is asking for access to the internet.
If you don't recognize this program, this is your chance to block it from reaching the network.

☐ Remember my decision

☑ Send this program to BullGuard for analysis

We do not feel this is optimal for non-expert users, especially as we had chosen the "quiet" operating mode during setup. The application control feature can be changed in the firewall settings to allow all programs after a specified period; this can be set to 0 seconds, meaning that programs will instantly be allowed access without a prompt appearing.

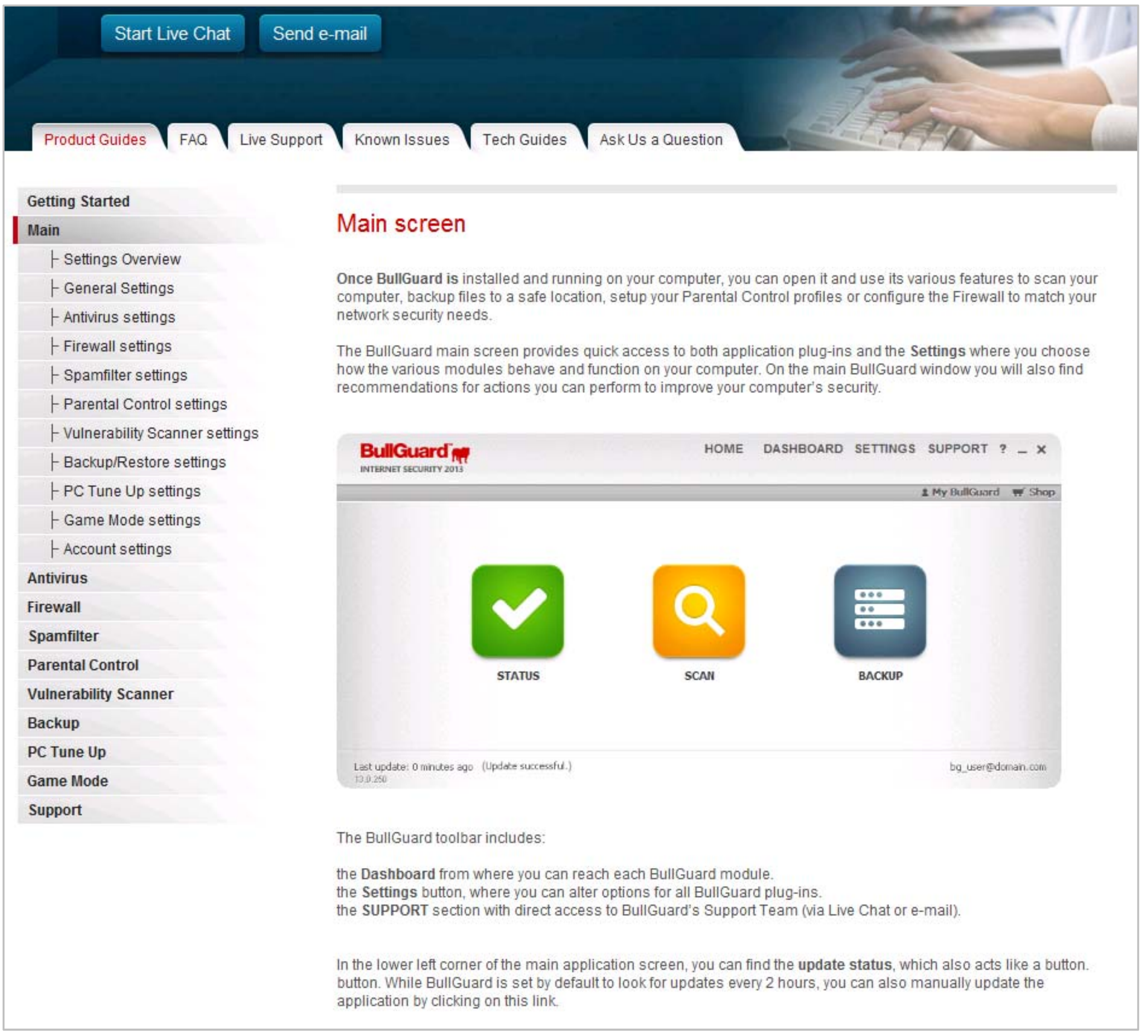
Safe Mode

When we started our test PC in Safe Mode with Networking, we were able to open the BullGuard Internet Security 2013 window, which appeared to be functioning exactly as normal, with the Status button showing "All is well". We wondered whether this might mean that real-time protection was functioning; however, we were able to download the EICAR test file without its content being stripped out, and copy our malware samples from one folder to another, thus demonstrating that RTP was in fact disabled. Again, BullGuard say this is scheduled for correction in the next release.

We were impressed to see that clicking the update link downloaded and installed the latest signature updates. We were able to run custom and context-menu scans and remove malware exactly as in standard mode.

Help and documentation

Clicking on the question-mark symbol in the top right-hand corner of BullGuard's main window opens the suite's online help page on the BullGuard website. This features a tree of functions and settings on the left-hand side of the page, with a detailed description of each one in the main panel on the right:



Main screen

Once BullGuard is installed and running on your computer, you can open it and use its various features to scan your computer, backup files to a safe location, setup your Parental Control profiles or configure the Firewall to match your network security needs.

The BullGuard main screen provides quick access to both application plug-ins and the **Settings** where you choose how the various modules behave and function on your computer. On the main BullGuard window you will also find recommendations for actions you can perform to improve your computer's security.

The BullGuard toolbar includes:

the **Dashboard** from where you can reach each BullGuard module.
the **Settings** button, where you can alter options for all BullGuard plug-ins.
the **SUPPORT** section with direct access to BullGuard's Support Team (via Live Chat or e-mail).

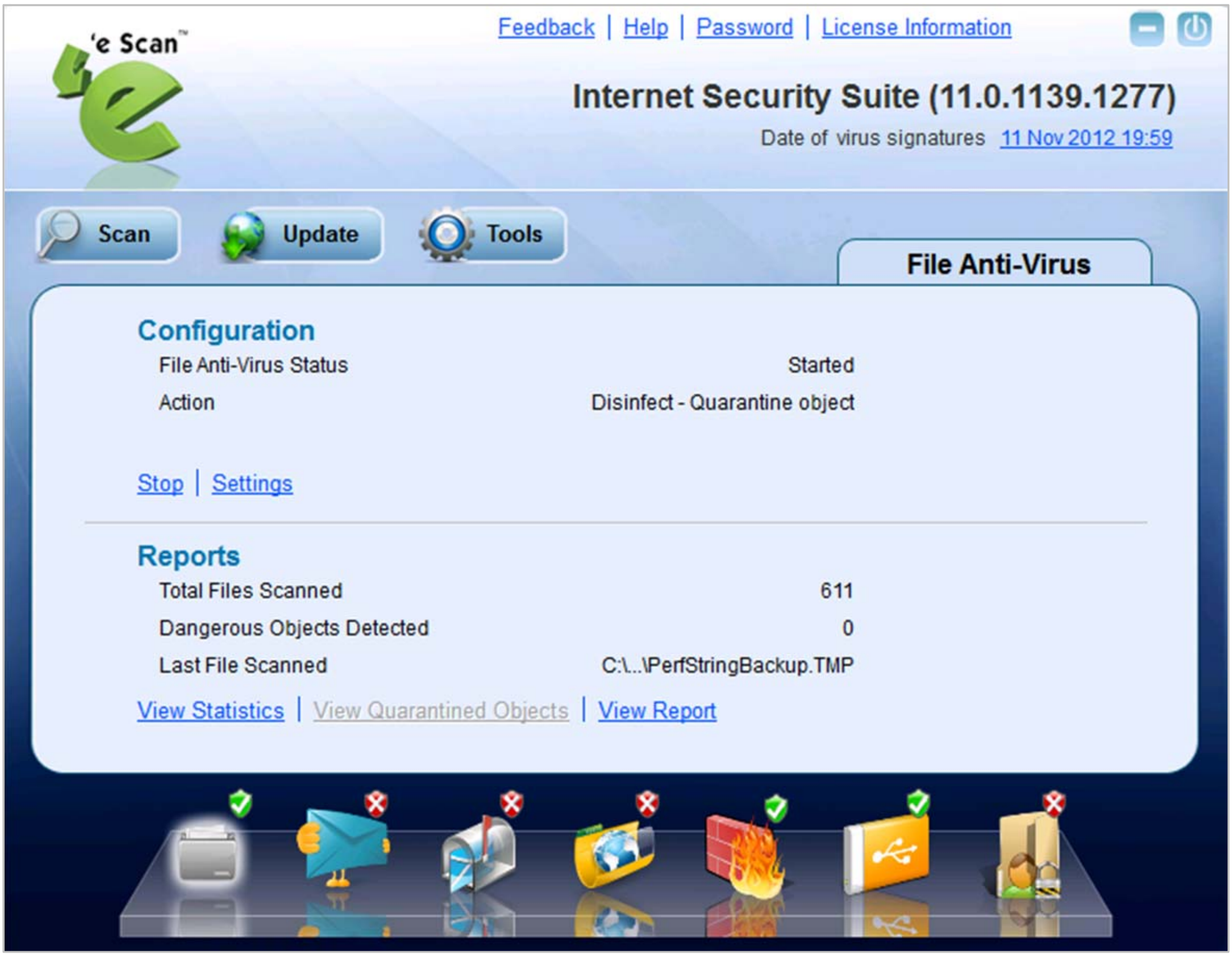
In the lower left corner of the main application screen, you can find the **update status**, which also acts like a button. button. While BullGuard is set by default to look for updates every 2 hours, you can also manually update the application by clicking on this link.

We found the explanations of each of the settings/functions pages to be very good, being clearly and comprehensively explained, and well illustrated with suitable screenshots. We were unable to find any sort of search function, however, so finding answers to our queries on scheduling a scan and settings scan exceptions involved looking for likely pages in the tree on the left, and then reading through each page in detail to try to find what we were looking for. We feel that a search function would make finding specific items quicker and easier, and understand that BullGuard are already developing a solution. We also note that whilst the instructions provided explain clearly how to use a particular dialog box in the program, they do not explain how to find that dialog in the first place. Whilst confident users will not find this a problem, we feel it could be made easier for non-experts by adding a quick explanation of which items to click on to get to the dialog box in question. We see that the online service can also be accessed by clicking the Support link (next to the question mark symbol on the home page) and then clicking Browse Help Topics. We were unable to find any form of local help or downloadable manual for BullGuard Internet Security 2013.

Verdict

We found the layout of BullGuard's program window to be very clean and simple, which ensures that non-expert users are not overloaded with information or functions. We did feel that some features, such as subscription information and custom scan options, were not very easy to find, however. Whilst default actions and alerts on malware discovery are good, we are concerned that real-time protection can be disabled using a non-administrator account, and that the program's warning of this can be permanently deactivated with a single click. Positive features include the ability to update the malware signatures in Safe Mode with Networking, and the co-ordination between the suite's firewall and Windows Network and Sharing Center. BullGuard's online help service is good as far as it goes, but we suggest it could be improved by a few additions such as a search function. We note that BullGuard are already developing solutions to many of the issues we found, and are impressed with their obvious commitment to product improvement.

eScan Internet Security 11.0



Internet Security Suite (11.0.1139.1277)

Date of virus signatures 11 Nov 2012 19:59

Configuration

File Anti-Virus Status	Started
Action	Disinfect - Quarantine object

Stop | Settings

Reports

Total Files Scanned	611
Dangerous Objects Detected	0
Last File Scanned	C:\...\PerfStringBackup.TMP

View Statistics | View Quarantined Objects | View Report

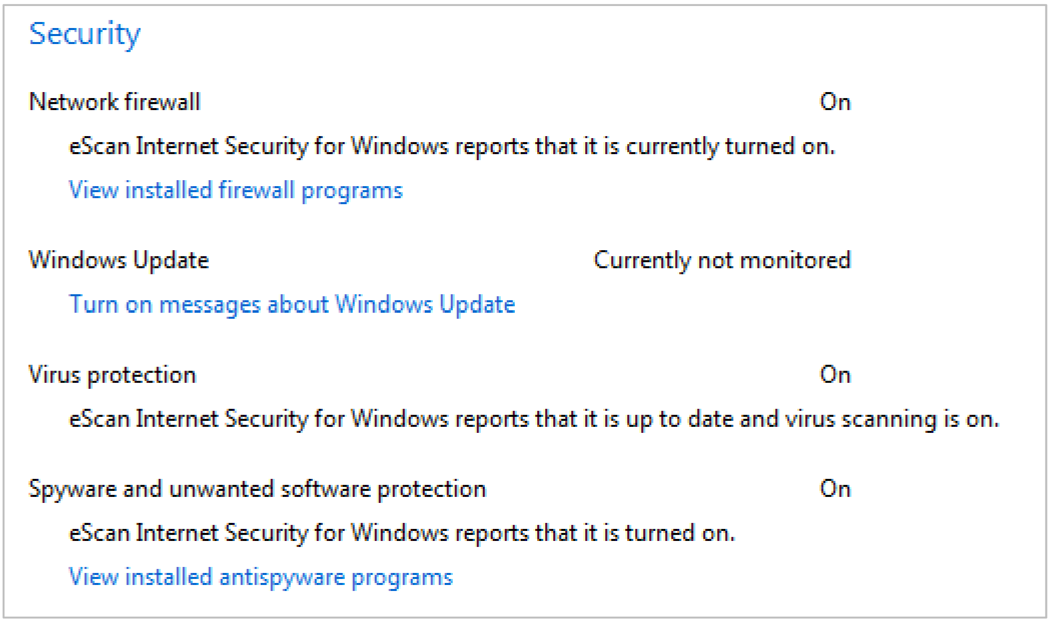
Components

eScan Internet Security 11 is a suite comprising antimalware functionality with email scanning, firewall and spam protection.

Installation

We downloaded a 190 MB full installation package, available on MicroWorld's website as a trial version. Installation was very simple, and involved just choosing a language (there is a range of European languages available), accepting the licence agreement, and choosing the installation folder location. There are no other options. At the end of the setup process, there is a warning to disable any other antivirus software on the PC, and a short scan (approx. 2 minutes) is run. The program does not ask about the type of network the PC is connected to, and a reboot is not required.

eScan Internet Security 11 registers itself in Windows 7's Action Center as an antivirus and antispyware program and firewall. It disables both Windows Firewall and Windows Defender.



Security

Network firewall On

eScan Internet Security for Windows reports that it is currently turned on.

View installed firewall programs

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

eScan Internet Security for Windows reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

eScan Internet Security for Windows reports that it is turned on.

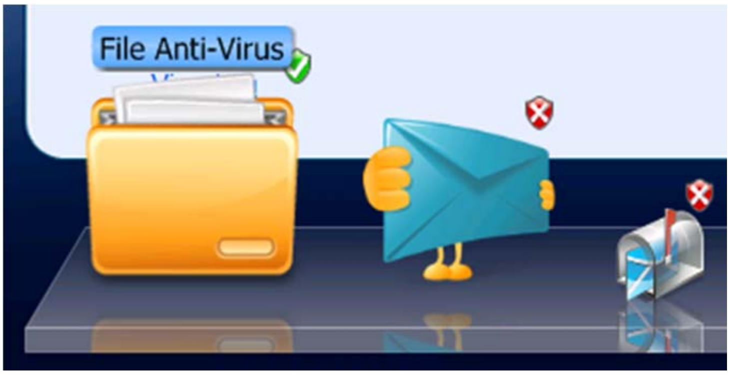
View installed antispyware programs

If eScan's real-time protection is disabled, Windows Action Center immediately shows its normal alert.

The uninstall program has no options at all, offering only complete removal.

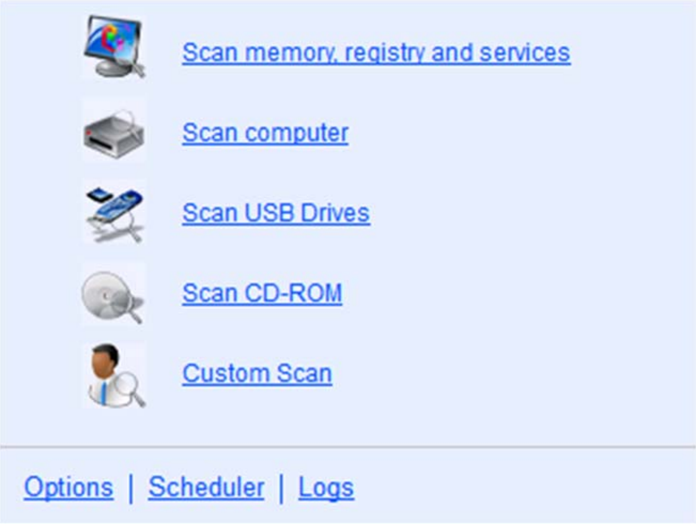
Program interface

eScan Internet Security 11 retains the window layout of previous versions, with a central information panel, and a row of very artistically designed icons along the bottom, representing the different protection components of the suite. We retain our reservations about how clear these icons would be to a new user of the suite, although we note that mousing over an icon enlarges it, and displays a caption with its function:

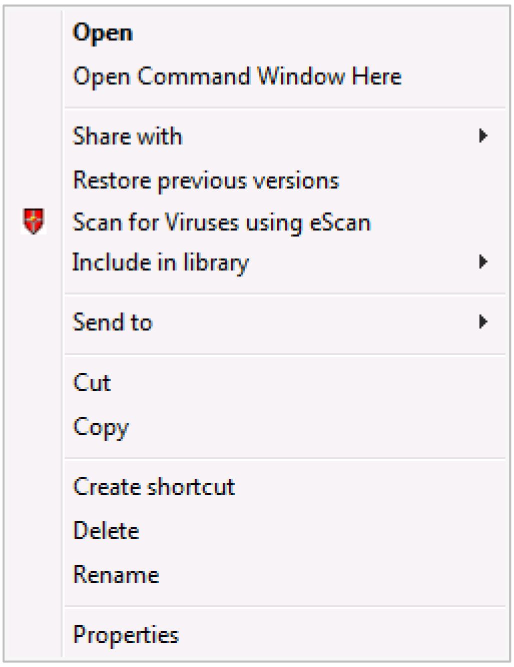


There is no kind of overall status display, and if a component such as real-time protection is disabled, in our opinion there is no very obvious warning that this has happened; the little green tick icon next to the File Anti-Virus icon turns to a red cross icon, and the Stop link in the configuration page turns to Start, but we feel neither of these could be described as an eye-catching alert (the program's system tray icon does show a red cross through it). Reactivating the component requires the user to go to the appropriate page and click the Start link.

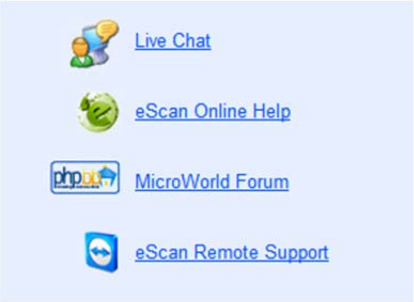
Updating and scanning are easily carried out using the very obvious Scan and Update buttons at the top of the program window. The Scan page offers a variety of different scan types:


Scan memory, registry and services
Scan computer
Scan USB Drives
Scan CD-ROM
Custom Scan
Options | Scheduler | Logs

eScan Internet Security integrates itself into Windows Explorer by means of a Scan entry in the context menu:



Subscription information can easily be seen by clicking on the License Information link at the top of the window. A link to the help features is found in the same place, and displays the available help options:



Default configuration

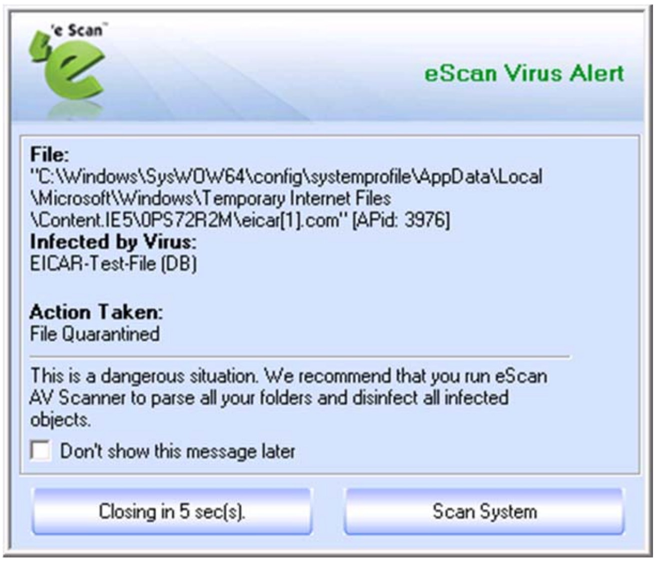
Non-administrator access

When we logged on to our test PC with a non-administrator account, we found that the settings links were all disabled, meaning that it was impossible to deactivate real-time protection or other important components. We regard this as optimal.

Scanning and malware discovery

A scheduled scan is not configured by default, but the Scan page has a link to the scheduler (see screenshot above), with which a scheduled scan can be set up. We could not find a means of running a boot-time scan.

When we attempted to download the EICAR test file, eScan blocked the download and displayed the following warning message:



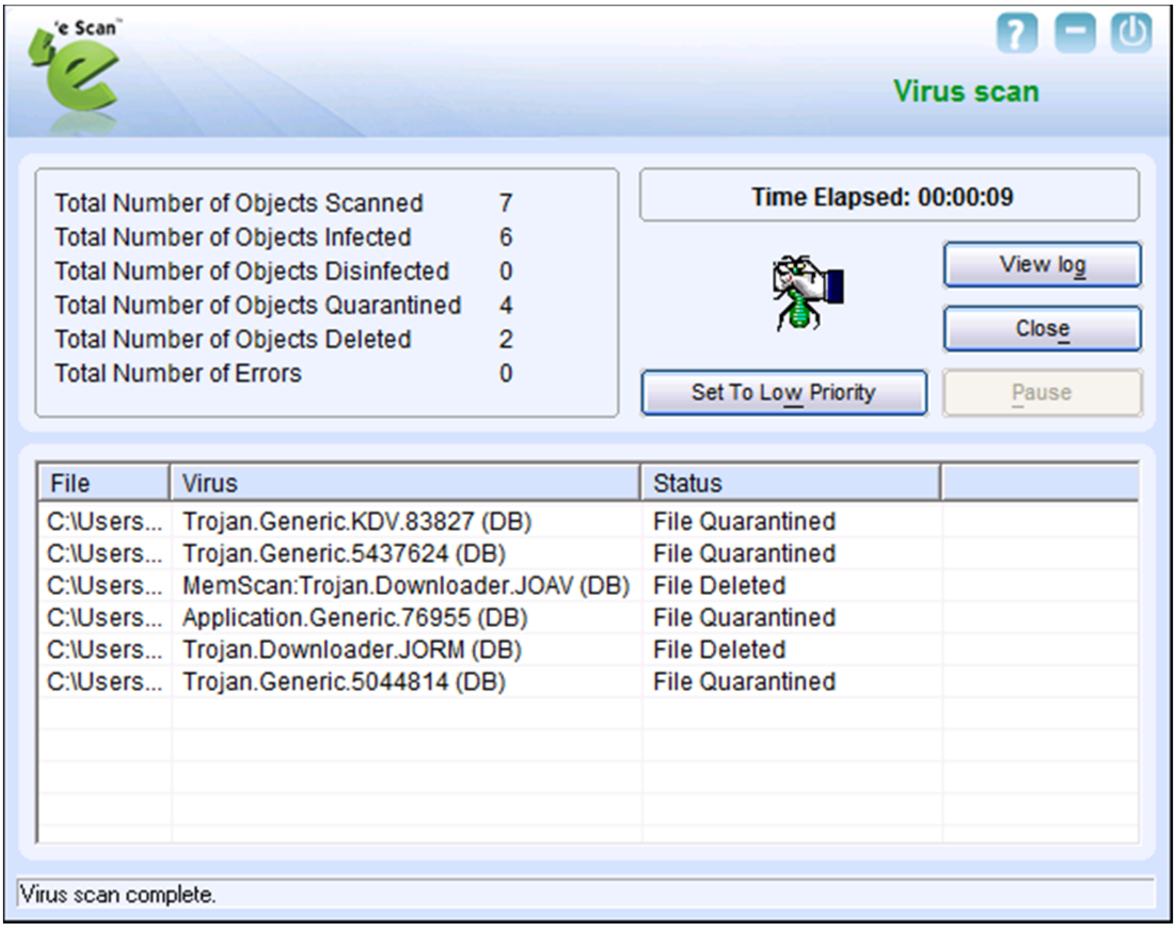
File:
"C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\0PS72R2M\eicar[1].com" [APid: 3976]
Infected by Virus:
EICAR-Test-File (DB)

Action Taken:
File Quarantined

This is a dangerous situation. We recommend that you run eScan AV Scanner to parse all your folders and disinfect all infected objects.

□ Don't show this message later

The message states clearly that the file has been quarantined. When malware was discovered by eScan's real-time protection, it was also quarantined, and a very similar message to the one above was displayed. When we scanned our folder of malware using either a custom scan from the console, or Windows Explorer's context menu, eScan quarantined or deleted all the items without any user intervention being required:



Time Elapsed: 00:00:09

Total Number of Objects Scanned	7
Total Number of Objects Infected	6
Total Number of Objects Disinfected	0
Total Number of Objects Quarantined	4
Total Number of Objects Deleted	2
Total Number of Errors	0

File	Virus	Status	
C:\Users...	Trojan.Generic.KDV.83827 (DB)	File Quarantined	
C:\Users...	Trojan.Generic.5437624 (DB)	File Quarantined	
C:\Users...	MemScan:Trojan.Downloader.JOAV (DB)	File Deleted	
C:\Users...	Application.Generic.76955 (DB)	File Quarantined	
C:\Users...	Trojan.Downloader.JORM (DB)	File Deleted	
C:\Users...	Trojan.Generic.5044814 (DB)	File Quarantined	

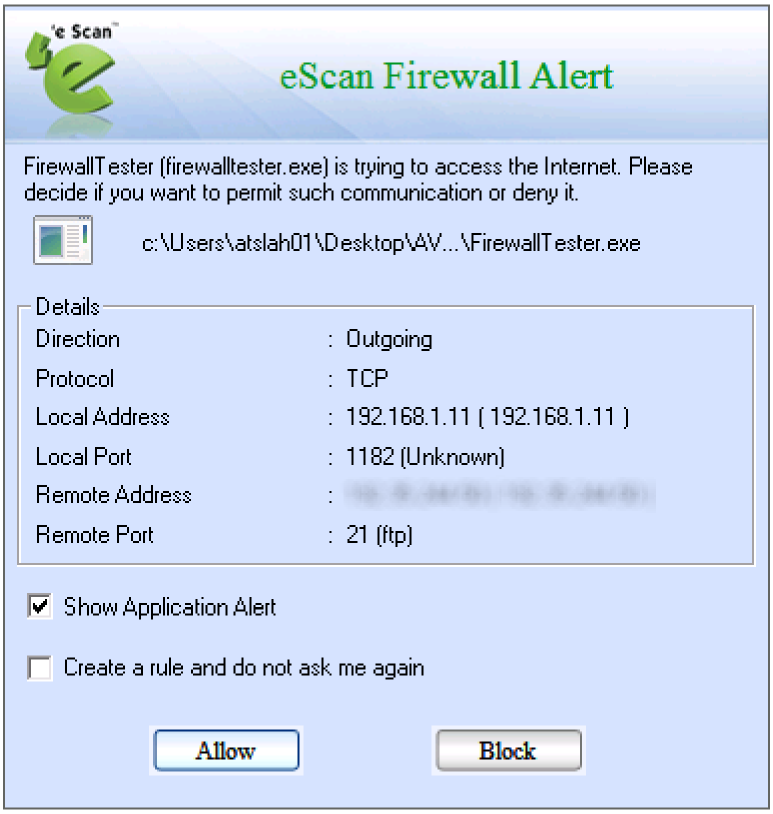
Virus scan complete.

Inbound firewall settings

After installation of eScan Internet Security 11, we were still able to ping our test PC, access its file share and log on via Remote Desktop, just as we had before installing the suite. When we changed the network type to Public in Windows' Network and Sharing Center, we found that eScan's firewall registered the change and accordingly blocked ping and file sharing access. Whilst this also blocked Remote Desktop access using the PC's hostname, we were able to log on to our test machine with Remote Desktop using its IP address. We are concerned that this may allow unauthorised access to the computer on a public network, and would urge eScan to investigate.

Outbound firewall/application control

In its default configuration, we found that the eScan firewall allowed our firewall tester to run and complete its download without any sort of query. Changing the firewall setting from the standard Limited Filter to Interactive Filter produced the following prompt when the firewall tester was run:



eScan Firewall Alert

FirewallTester (firewalltester.exe) is trying to access the Internet. Please decide if you want to permit such communication or deny it.

c:\Users\atslah01\Desktop\AV...\FirewallTester.exe

Details

Direction	:	Outgoing
Protocol	:	TCP
Local Address	:	192.168.1.11 (192.168.1.11)
Local Port	:	1182 (Unknown)
Remote Address	:	[redacted]
Remote Port	:	21 (ftp)

☑ Show Application Alert

□ Create a rule and do not ask me again

Safe Mode

When we started our test PC in Safe Mode with Networking, we found that no scanning or update controls were available from the main program window of eScan Internet Security 11. However, we were able to run a context-menu scan of our malware folder; this functioned exactly as it would in standard mode, and deleted or quarantined all the malware samples.

Help and documentation

There is no local help function in eScan Internet Security 11, but there is an obvious link on the Help page to eScan Online Help. This opens a browser window on an apparently random "eScan Wikipedia" page, which displays a description of the functions available in the main program window (which we felt was rather confusing). We could not find an obvious means of showing an overview, or progressing to other pages. Using the Search function on this page to look for answers to our queries on scan exclusions and scheduled scans proved to be pointless; very few results were returned, and these had simply picked up on the text string "scan" as found in the product's name, eScan.

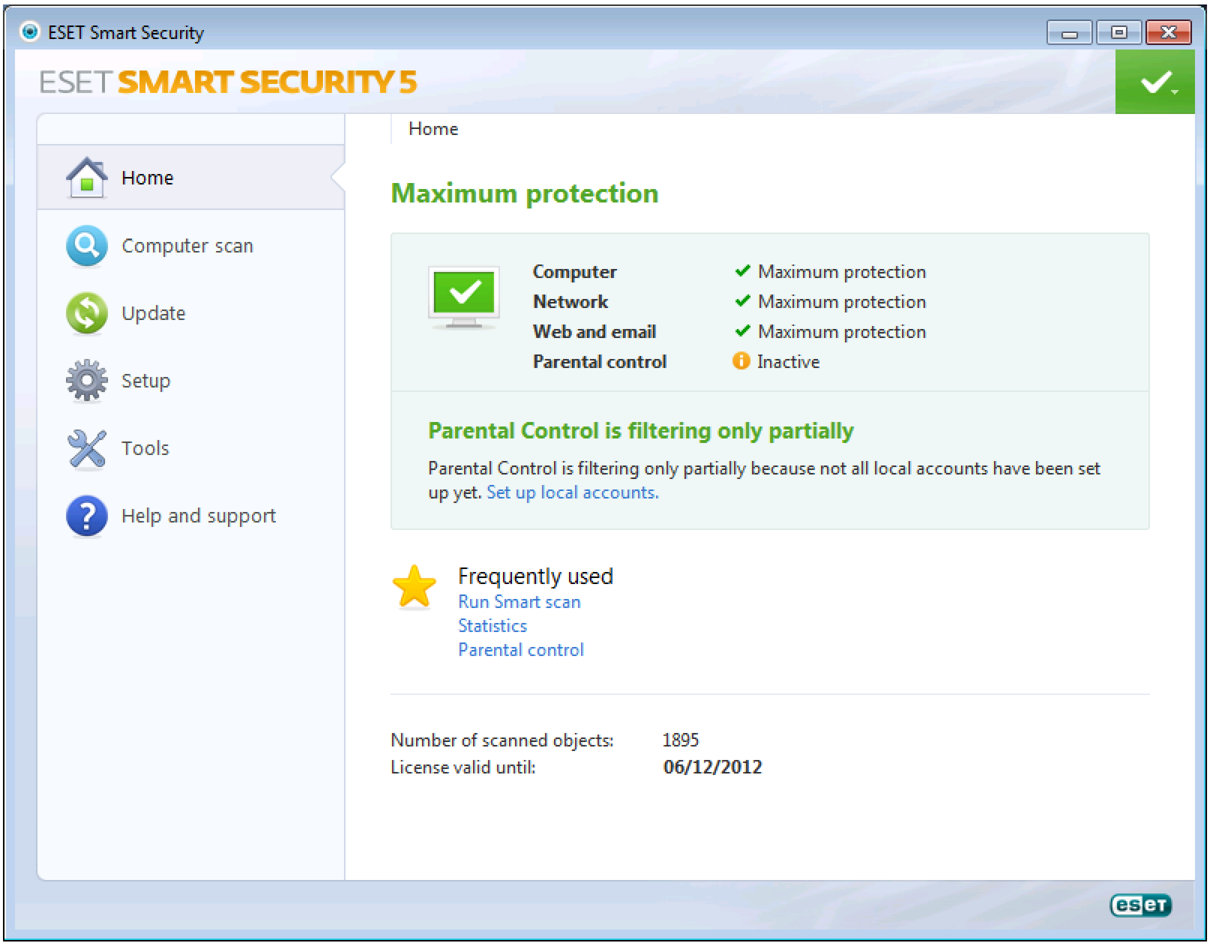
The page also had a link to the Knowledge Base, which we clicked. This took us to an overview page with more links, including FAQs and the “Online Guide for Windows-based Products”. The FAQs were also of limited value; the first two questions in the section “eScan Configuration” are: “1. What is Rule-Set?” and “2. How does Rule-Set get updated?”. The section entitled “eScan How To FAQs” contains precisely one question: “1. How to update MWAV utility?”. Many of the FAQs appear to apply only to the business version of the product. Clicking on “Online Guide for Windows-based Products” finally took us to an overview page, listing components and functions of the suite such as File-Antivirus, Scan, and Update; clicking on an item opened a page describing its configuration. This was useful, but in many cases the content was more or less identical to the manual described below. Overall, we can only describe our experience with the online help for eScan Internet Security as confusing and frustrating.

MicroWorld have produced a comprehensive 116-page manual for eScan Internet Security, which can easily be downloaded from their website. It contains fairly detailed instructions for installing, configuring and using the product. It is abundantly illustrated with screenshots, although these are not of the highest resolution. The format of the document is simple but clear and readable. Unfortunately, the contents page is very brief, without links to the pages, and there are no bookmarks. This means the document can only be navigated using Adobe Reader’s Thumbnails bar. We were able to find answers in the manual (albeit not very detailed) to our queries on scheduling a scan and setting scan exceptions.

Verdict

We found eScan Internet Security 11 to be a functional suite that performs as it should. Installation is very straightforward, and default settings are sensible. However, we still have reservations about the clarity of the interface, and feel that some aspects of it are rather confusing, especially for non-expert users. Whilst the user’s manual is of an acceptable standard, we would suggest that the online help function could be very much improved. For these reasons, we regard the suite as being better suited to advanced users than to non-experts.

ESET Smart Security 5.2



Home

Maximum protection

Computer	✓ Maximum protection
Network	✓ Maximum protection
Web and email	✓ Maximum protection
Parental control	Inactive

Parental Control is filtering only partially

Parental Control is filtering only partially because not all local accounts have been set up yet. Set up local accounts.

Frequently used
Run Smart scan
Statistics
Parental control

Number of scanned objects: 1895
License valid until: 06/12/2012

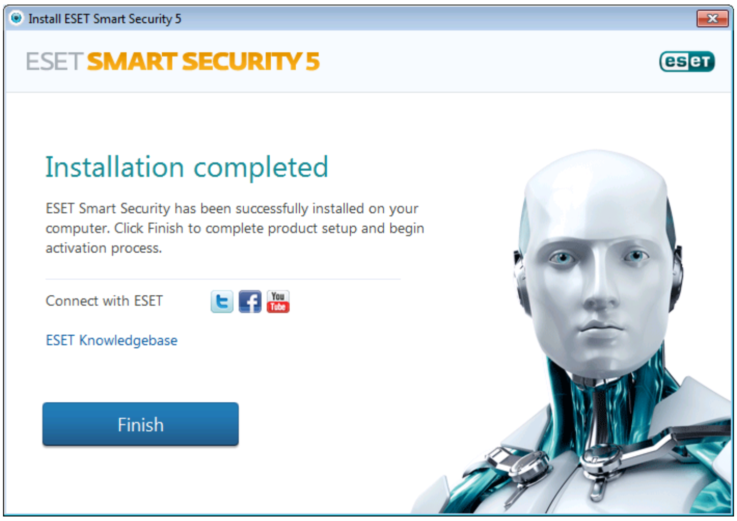
Components

ESET Smart Security 5 consists of an antimalware component with email protection, a firewall, spam protection, and parental controls.

Installation

We installed ESET Smart Security 5 from a 1.3 MB downloader file provided for the trial (a 60 MB full installer can also be freely downloaded from the website, and this includes a custom installation option). There is no custom setup option in the downloader as such, but the wizard provides sensible options for changing some settings, and these are well explained. There is no means of selecting the components to be installed at this stage (although later deactivation is possible). The wizard provides a one-time choice of the language to be used for the installation and program interface; there is a wide range of European languages and a few Asian ones.

Steps in the wizard include accepting a licence agreement, choosing whether to participate in Live Grid (ESET's malware information sharing service), installation folder location, and whether or not the suite should guard against potentially unwanted programs. Helpful, the final page of the wizard includes a link to ESET's knowledgebase:



Install ESET Smart Security 5

ESET SMART SECURITY 5

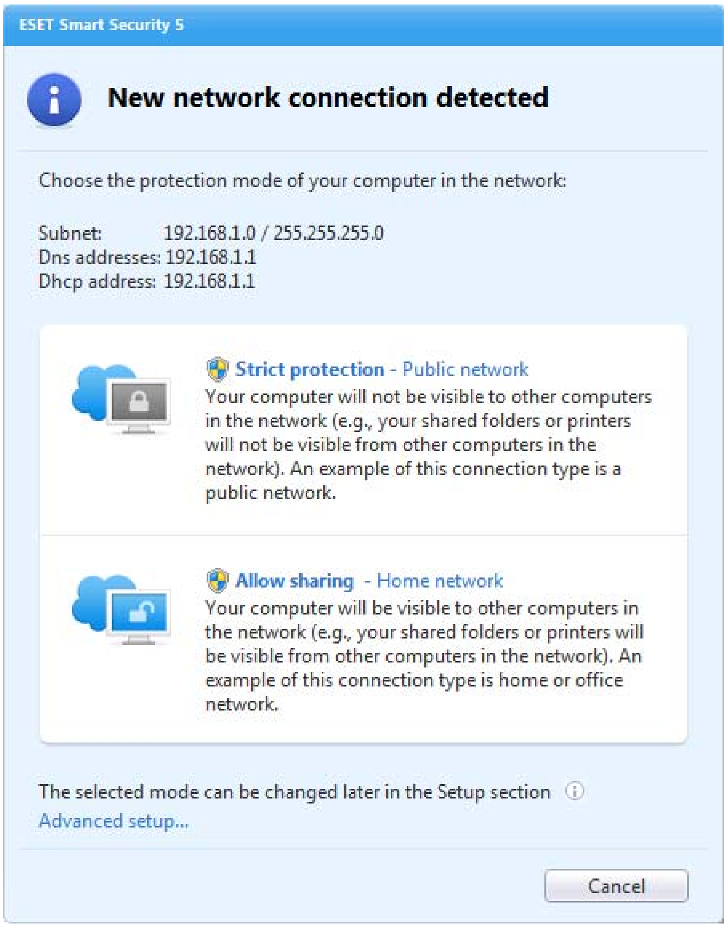
Installation completed

ESET Smart Security has been successfully installed on your computer. Click Finish to complete product setup and begin activation process.

Connect with ESET

ESET Knowledgebase

When Finish has been clicked, a dialog box appears, asking whether the current network should be regarded as public or private. There is a description of each of the possibilities, which we found useful:



ESET Smart Security 5

New network connection detected

Choose the protection mode of your computer in the network:

Subnet: 192.168.1.0 / 255.255.255.0
Dns addresses: 192.168.1.1
Dhcp address: 192.168.1.1

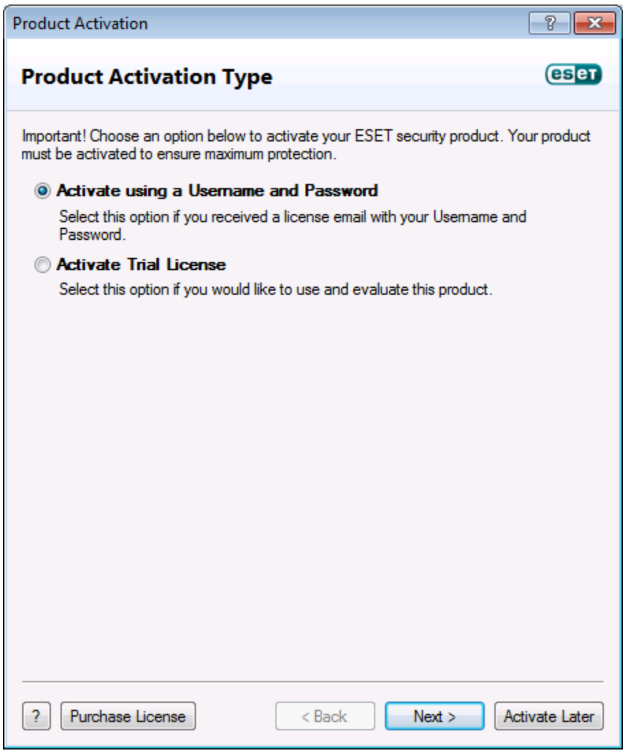
Strict protection - Public network
Your computer will not be visible to other computers in the network (e.g., your shared folders or printers will not be visible from other computers in the network). An example of this connection type is a public network.

Allow sharing - Home network
Your computer will be visible to other computers in the network (e.g., your shared folders or printers will be visible from other computers in the network). An example of this connection type is home or office network.

The selected mode can be changed later in the Setup section

Advanced setup...

When the program is opened, the activation wizard starts. This provides the option of entering a purchased key, or using the product as a 30-day trial:



Product Activation

Product Activation Type

Important! Choose an option below to activate your ESET security product. Your product must be activated to ensure maximum protection.

● **Activate using a Username and Password**

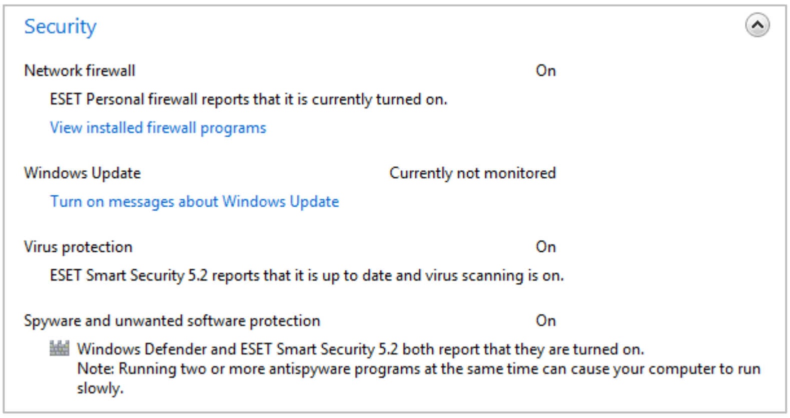
Select this option if you received a license email with your Username and Password.

○ **Activate Trial License**

Select this option if you would like to use and evaluate this product.

An email address has to be entered to register for the trial. Rebooting the computer was not required.

Windows Action Center reports that ESET Smart Security has registered itself as an antivirus and antispyware program and firewall. Windows Firewall has been disabled, but Windows Defender continues to run:



Security

Network firewall On

ESET Personal firewall reports that it is currently turned on.

View installed firewall programs

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

ESET Smart Security 5.2 reports that it is up to date and virus scanning is on.

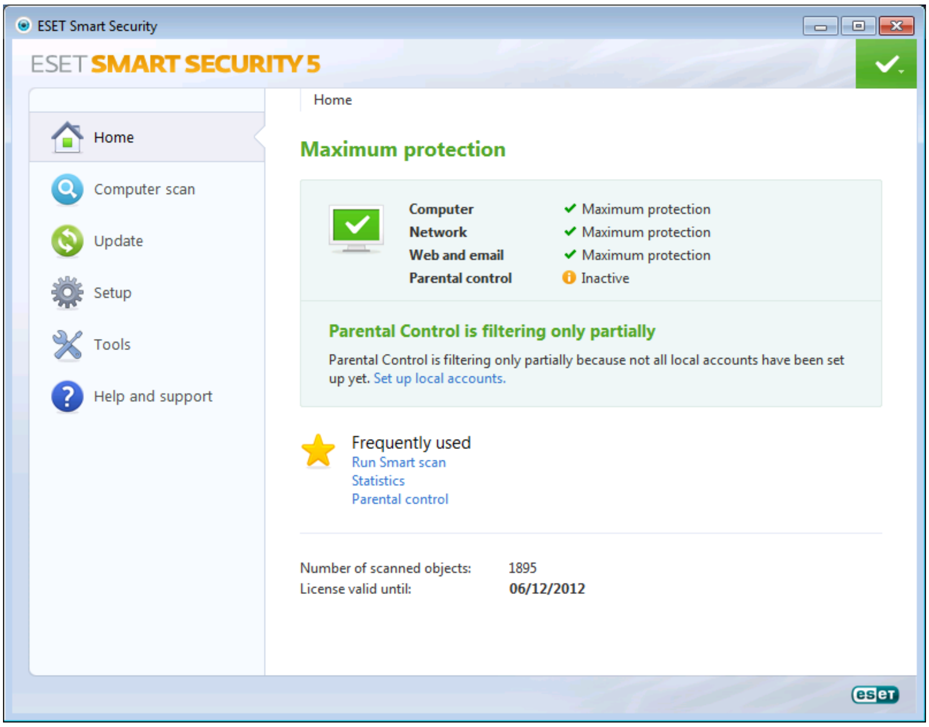
Spyware and unwanted software protection On

Windows Defender and ESET Smart Security 5.2 both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

If the real-time protection component is disabled, Windows Action Center immediately displays a warning.

The uninstaller program offers a choice of repairing the suite, or complete removal. There is no means of uninstalling individual components; however, the program's own settings allow both the firewall and the parental control components to be completely deactivated, which has exactly the same effect as uninstalling them.

Program interface



Maximum protection

Computer	✓ Maximum protection
Network	✓ Maximum protection
Web and email	✓ Maximum protection
Parental control	! Inactive

Parental Control is filtering only partially

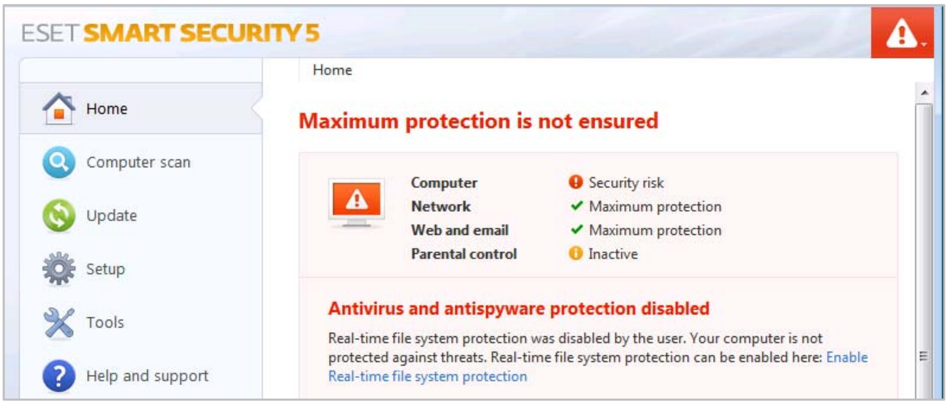
Parental Control is filtering only partially because not all local accounts have been set up yet. Set up local accounts.

Frequently used
Run Smart scan
Statistics
Parental control

Number of scanned objects:	1895
License valid until:	06/12/2012

Smart Security 5 retains the familiar interface of the previous version, consisting of a narrow left-hand pane with menu items, and a larger display panel on the right with the relevant information/configuration options. The Home page provides a status display and subscription information. Status is shown by a prominent title at the top; if all is well, this reads “Maximum protection”, and a tick (checkmark) symbol is displayed. Additionally, the status of the individual components is shown. We were pleased to note that the status display clearly points out that the parental control component has not been configured yet, and provides a link to do this. This would prevent parents from simply assuming that parental controls had already been set up.

If e.g. real-time protection is disabled, clear warnings are shown in red (text and exclamation mark symbol), informing the user which component has caused the alert, and providing a link to reactivate it:



Maximum protection is not ensured

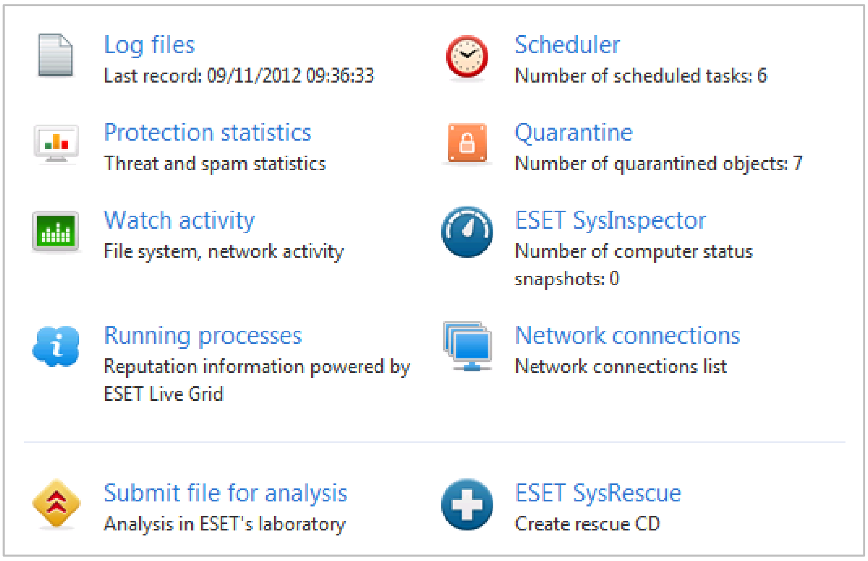
Computer	! Security risk
Network	✓ Maximum protection
Web and email	✓ Maximum protection
Parental control	! Inactive

Antivirus and antispyware protection disabled

Real-time file system protection was disabled by the user. Your computer is not protected against threats. Real-time file system protection can be enabled here: Enable Real-time file system protection

Update and scan functions are easily accessible from the obvious menu buttons on the left-hand side of the window. Other items include Setup, Tools, plus Help and Support. The Scan page has two main options, Smart Scan (full system) and Custom Scan. Setting up a scheduled scan is performed by going to the Tools Page and clicking Scheduler; we would suggest that a link to this on the Computer Scan page would be a helpful addition. We were unable to find any means of running a boot-time scan, but the Computer Scan Setup link on the Computer Scan page has a link to the detailed scan options, where a startup (logon) scan can be configured.

The Setup page displays individual sub-components of the suite (e.g. HIPS, Gamer Mode) and allows these to be configured. The Tools page provides logs, statistics, quarantine, ESET's System Inspector (detailed system information), advanced system monitoring tools, quarantine, the scheduler, plus the opportunities to submit suspicious files and burn a rescue disk:



Log files
Last record: 09/11/2012 09:36:33

Scheduler
Number of scheduled tasks: 6

Protection statistics
Threat and spam statistics

Quarantine
Number of quarantined objects: 7

Watch activity
File system, network activity

ESET SysInspector
Number of computer status snapshots: 0

Running processes
Reputation information powered by ESET Live Grid

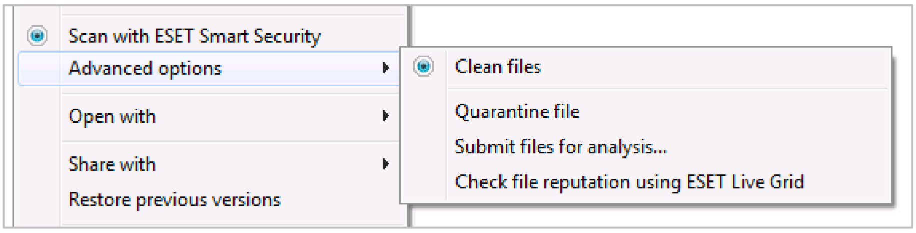
Network connections
Network connections list

Submit file for analysis
Analysis in ESET's laboratory

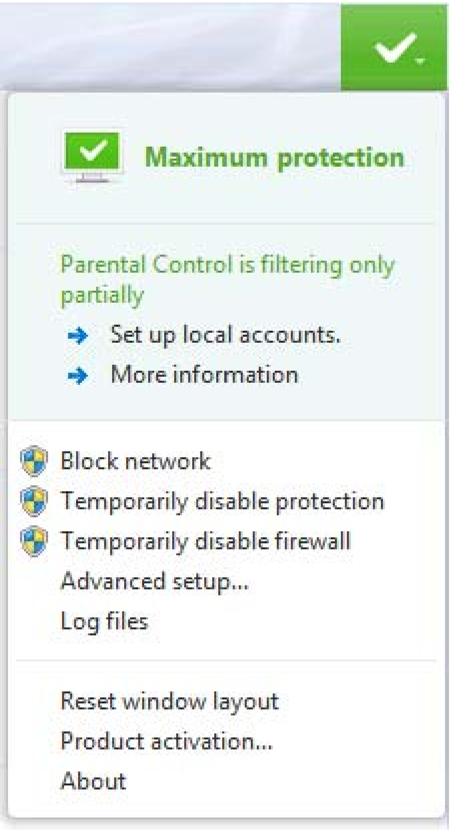
ESET SysRescue
Create rescue CD

The Help and Support page provides links to local and online support options, Customer Care Support Requests, and ESET's Threat Encyclopedia.

ESET Smart Security integrates itself into Windows Explorer's context menu by means of the following entries:


Scan with ESET Smart Security
Advanced options
Open with
Share with
Restore previous versions
Clean files
Quarantine file
Submit files for analysis...
Check file reputation using ESET Live Grid

A final feature of Smart Security's interface is the menu, which can be found by clicking on the button in the top right-hand corner of the window (which also doubles as a status icon):



Maximum protection

Parental Control is filtering only partially

We have noted the clarity and simplicity of ESET's main program window in reviews of the previous version, and are pleased to see that the same user-friendly design has been retained for the current incarnation.

Default configuration

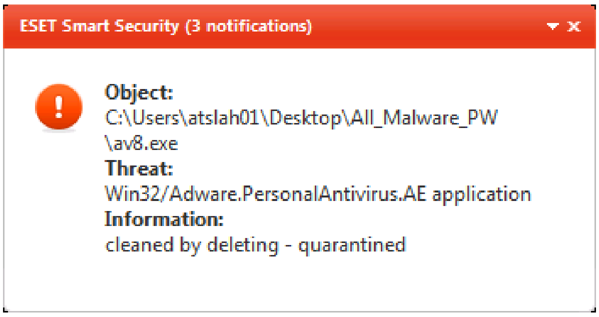
Non-administrator access

When we logged on to our test PC with a non-administrator account and attempted to disable the real-time protection, we were confronted with a Windows User Account Control prompt; without entering administrator credentials, we were unable to make any such configuration changes. This is optimal e.g. for parents who want to ensure their children cannot accidentally disable the protection.

Scanning and malware discovery

A scheduled scan is not configured by default, but can be set up using the Scheduler item on the Tools page. Whilst this would not present experienced users with any difficulty, we would suggest that it could be made a little friendlier for non-experts.

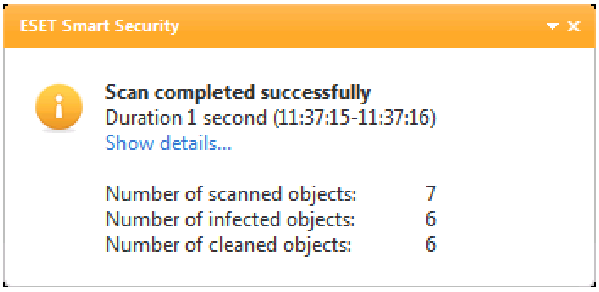
When malware is discovered by the suite's real-time protection, it is immediately deleted and the following message displayed:



ESET Smart Security (3 notifications)

Object:
C:\Users\atslah01\Desktop\All_Malware_PW
\av8.exe
Threat:
Win32/Adware.PersonalAntivirus.AE application
Information:
cleaned by deleting - quarantined

If a scan is run from the console, the malware is again cleaned, and again the message box makes this clear:

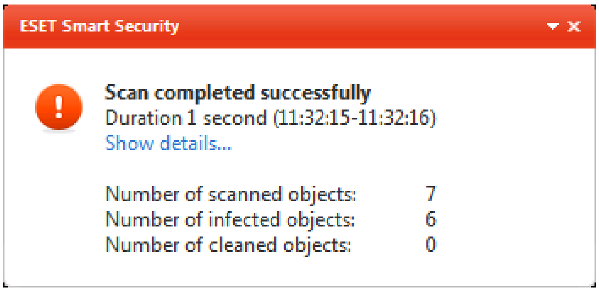


ESET Smart Security

Scan completed successfully
Duration 1 second (11:37:15-11:37:16)
Show details...

Number of scanned objects:	7
Number of infected objects:	6
Number of cleaned objects:	6

Unfortunately, scanning a folder containing malware files using the obvious "Scan with ESET Smart Security" entry on Windows Explorer's context menu still (as in previous versions) merely notes the number of malware items found, without taking any action, or giving the user any opportunity to quarantine or delete the malware found:



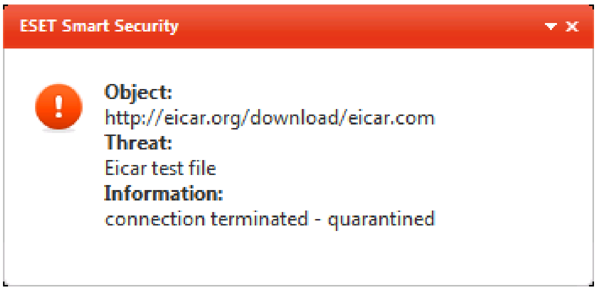
ESET Smart Security

Scan completed successfully
Duration 1 second (11:32:15-11:32:16)
Show details...

Number of scanned objects:	7
Number of infected objects:	6
Number of cleaned objects:	0

We remain baffled as to why ESET continue to use this configuration as the default, without even labelling it as e.g. "Scan without cleaning".

When we attempted to download the EICAR test file, ESET Smart Security blocked the download and displayed the following message:



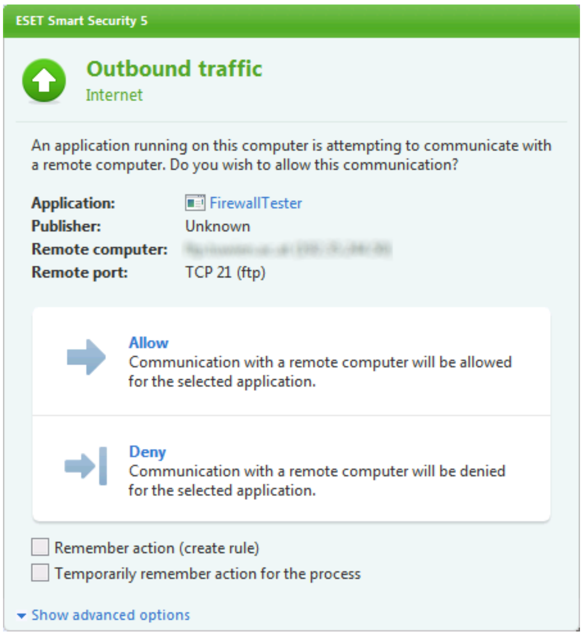
Object:
http://eicar.org/download/eicar.com
Threat:
Eicar test file
Information:
connection terminated - quarantined

Inbound firewall settings

As already noted, the setup routine concludes by asking the user whether it should configure the firewall for a private or public network. We chose private at this point, and were pleased to find that we were still able to ping our test PC, access the file share and control it by Remote Desktop afterwards. Changing the network type to public (Strict Protection) immediately blocked ping, RDP and file-sharing access. We note that ESET Smart Security always prompts for the network type when the computer is connected to a new network; however, if the network type is changed from Private to Public in Windows' Network and Sharing Center (as if the user had made a mistake), Smart Security does not prompt for the network type again. In this case, the user would need to change the network type in Smart Security's settings as well.

Outbound firewall/application control

The default settings in ESET Smart Security allowed our firewall testing program to access the Internet without any restrictions or queries, which we regard as optimal. It is possible to change this, as some advanced users may wish, by setting the firewall mode to Interactive. The following dialog box then appeared when the firewall tester was run:


ESET Smart Security 5
Outbound traffic
Internet

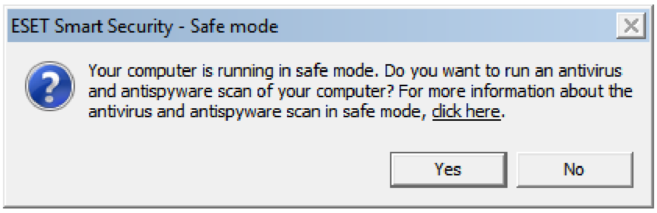
An application running on this computer is attempting to communicate with a remote computer. Do you wish to allow this communication?

Application: FirewallTester
Publisher: Unknown
Remote computer: [redacted]
Remote port: TCP 21 (ftp)

Allow
Communication with a remote computer will be allowed for the selected application.
Deny
Communication with a remote computer will be denied for the selected application.
□ Remember action (create rule)
□ Temporarily remember action for the process
Show advanced options

Safe Mode

Trying to open the GUI of ESET Smart Security in Safe Mode with Networking opened the following dialog box:



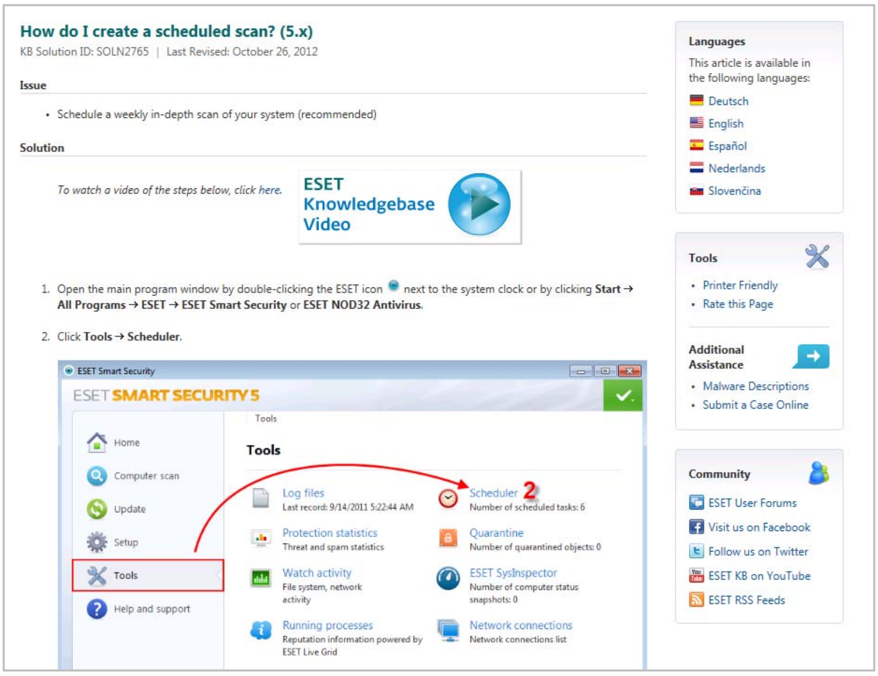
ESET Smart Security - Safe mode

Your computer is running in safe mode. Do you want to run an antivirus and antispyware scan of your computer? For more information about the antivirus and antispyware scan in safe mode, click here.

This allowed us to run a full system scan (a Command Prompt windows is displayed), which completely removed our malware samples. There was no option to update the virus signatures or run a custom scan; the context-menu scan item was inoperative, as was real-time protection . However, we note that a rescue disk can be made from the ESET SysRescue item in Tools, and that this allows both updating and custom scans.

Help and documentation

We were easily able to find answers to our two queries, namely scheduling a scan and setting scan exclusions, from the local help. The scan exclusion instructions were particularly well explained and included a very helpful screenshot. The answer for our question on scheduling a scan related to scheduled tasks in general, not specifically a scan; we feel that specific instructions for this would be helpful for non-expert users. However, the online help function, accessed by clicking "Search Internet Knowledgebase" on the Help page, provided exactly the directions we were looking for: a simple, clear, step-by-step guide to scheduling a scan, perfectly illustrated at every stage with annotated screenshots:



How do I create a scheduled scan? (5.x)

KB Solution ID: SOLN2765 | Last Revised: October 26, 2012

Issue

- Schedule a weekly in-depth scan of your system (recommended)

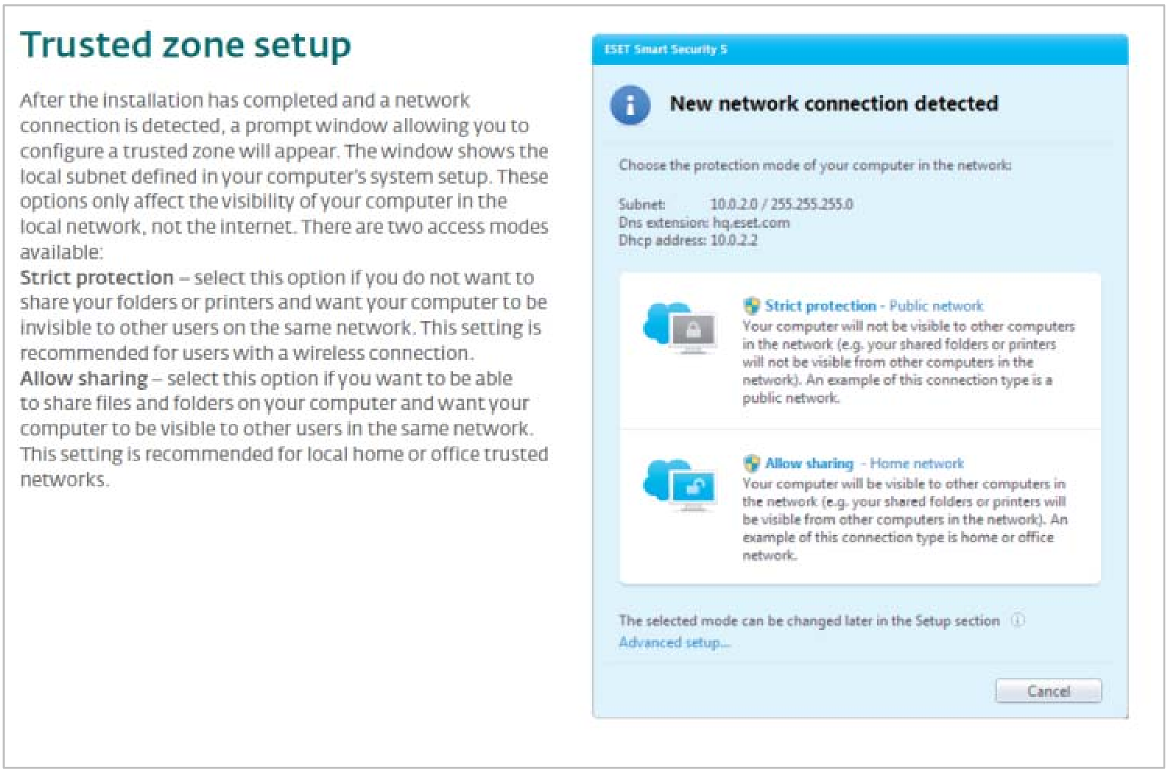
Solution

To watch a video of the steps below, click here.

1. Open the main program window by double-clicking the ESET icon next to the system clock or by clicking **Start → All Programs → ESET → ESET Smart Security** or **ESET NOD32 Antivirus**.
2. Click **Tools → Scheduler**.

We note that there is even a video available for this task. The Knowledge Base instructions for setting scan exclusions were also of the same exemplary standard.

Two manuals for Smart Security 5 can easily be downloaded from ESET's website, a 12-page Quick Start Guide, and a 118-page User Guide. The Quick Start Guide covers the essentials of installation and maintenance, in a very simple format which we found to be ideal. The screenshot below represents one entire page of the document:



Trusted zone setup

After the installation has completed and a network connection is detected, a prompt window allowing you to configure a trusted zone will appear. The window shows the local subnet defined in your computer's system setup. These options only affect the visibility of your computer in the local network, not the internet. There are two access modes available:
Strict protection – select this option if you do not want to share your folders or printers and want your computer to be invisible to other users on the same network. This setting is recommended for users with a wireless connection.
Allow sharing – select this option if you want to be able to share files and folders on your computer and want your computer to be visible to other users in the same network. This setting is recommended for local home or office trusted networks.

New network connection detected

Choose the protection mode of your computer in the network:

Subnet: 10.0.2.0 / 255.255.255.0
Dns extension: hq.eset.com
Dhcp address: 10.0.2.2

Strict protection - Public network
Your computer will not be visible to other computers in the network (e.g. your shared folders or printers will not be visible from other computers in the network). An example of this connection type is a public network.

Allow sharing - Home network
Your computer will be visible to other computers in the network (e.g. your shared folders or printers will be visible from other computers in the network). An example of this connection type is home or office network.

The selected mode can be changed later in the Setup section
Advanced setup...

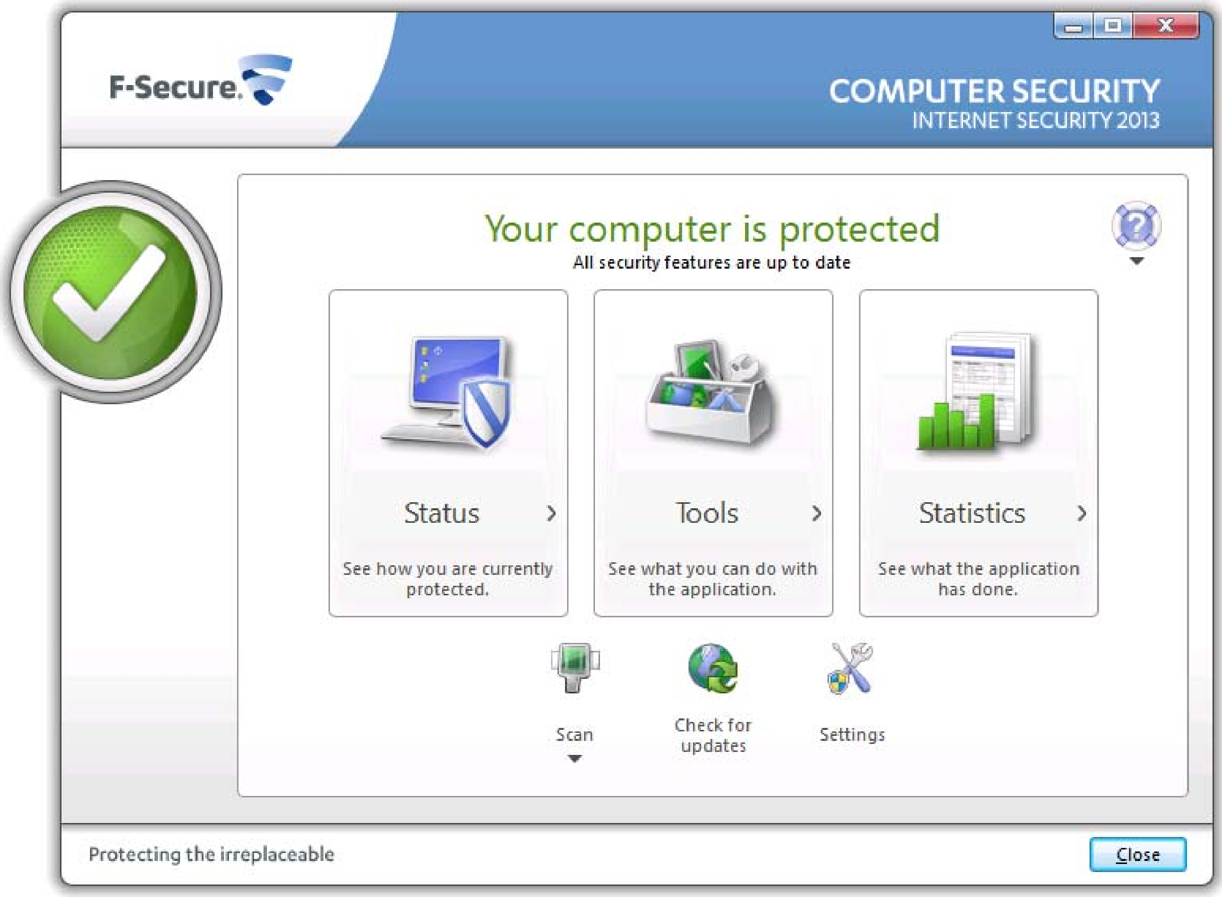
The User Guide has been comprehensively indexed and bookmarked, providing one-click access to any section via the contents page or Adobe Reader Bookmarks Bar, as is appropriate for a document of that length. It has been clearly written, well organised, and very well illustrated with screenshots. We can only describe ESET's documentation as outstanding.

Verdict

In our opinion, this year's version of ESET Smart Security retains the remarkably simple and clear layout of previous versions, with sensible default settings and clear warning/information messages. We were pleased to see that ESET have adopted a suggestion we made last year by clearly showing that parental controls need to be configured before they become effective. The documentation and online knowledge base continue to be of an exemplary standard.

Our one significant suggestion for improvement is to provide the default context-menu scan with an option for removing the malware it has found.

F-Secure Internet Security 2013



F-Secure.

COMPUTER SECURITY
INTERNET SECURITY 2013

Your computer is protected
All security features are up to date

Status ›
See how you are currently protected.
Tools ›
See what you can do with the application.
Statistics ›
See what the application has done.
Scan
Check for updates
Settings

Protecting the irreplaceable

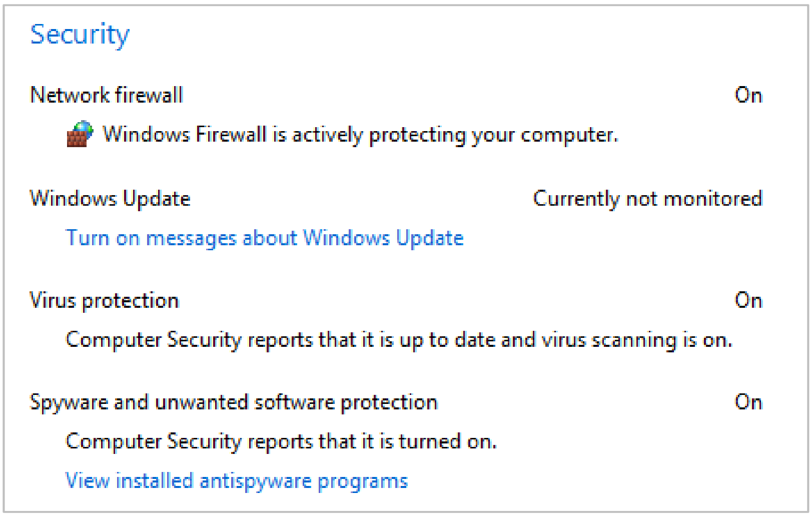
Components

F-Secure Internet Security 2013 comprises an antimalware component with antispam (together these are called Computer Security), and parental controls (called Online Safety). Please note that the 2013 version of the suite uses Windows Firewall; as noted in the introduction to this report, we do not regard this as being any sort of disadvantage.

Installation

We installed F-Secure Internet Security 2013 from a 1 MB downloader file which is provided for the trial version. Steps in the setup wizard include a choice of major European languages, opting in or out of malware data sharing, and accepting the licence agreement. There is no choice of components. A reboot was not required.

F-Secure Internet Security 2013 registers itself in Windows Action Center as an antivirus and antispyware program. Windows Defender is disabled, Windows Firewall is not:



Security

Network firewall On

Windows Firewall is actively protecting your computer.

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

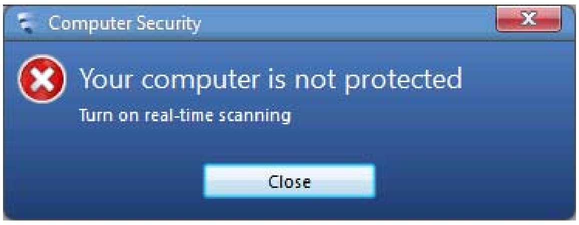
Computer Security reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

Computer Security reports that it is turned on.

View installed antispyware programs

We remain surprised that F-Secure does not display its own name in the Action Center; we feel that "F-Secure Computer Security" would be more reassuring to users, and surely good advertising for the company. If F-Secure's real-time protection is disabled, Windows Action Center displays its normal alert. Additionally, F-Secure shows its own warning message, which is more obvious and more persistent than Action Center's:



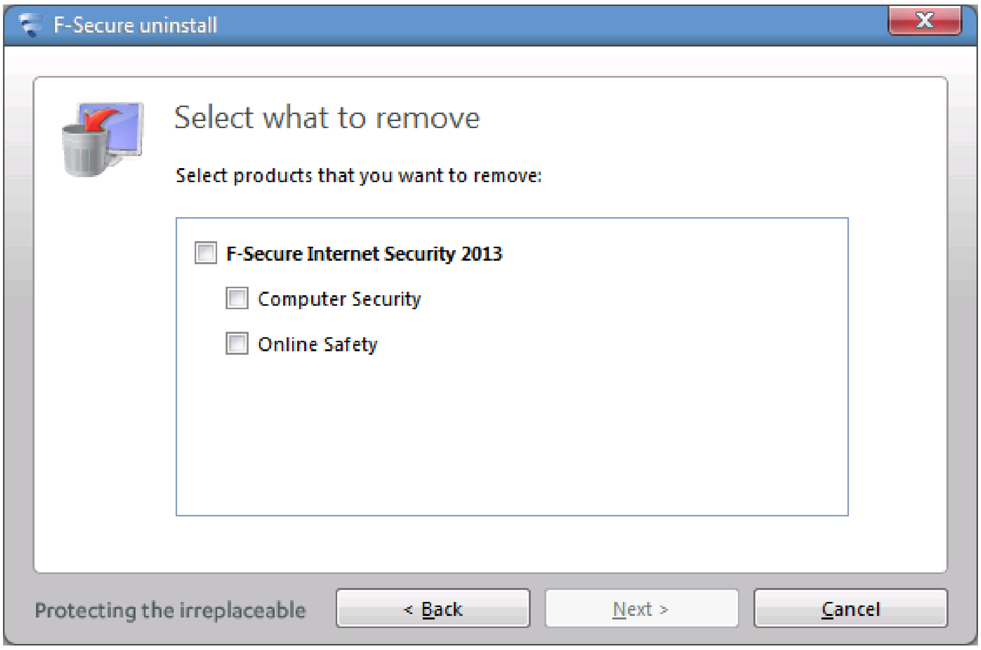
Computer Security

Your computer is not protected

Turn on real-time scanning

We feel this warning is a valuable addition.

The program's uninstaller has a Change option, which allows selective removal of the suite's two main components:



F-Secure uninstall

Select what to remove

Select products that you want to remove:

□ F-Secure Internet Security 2013

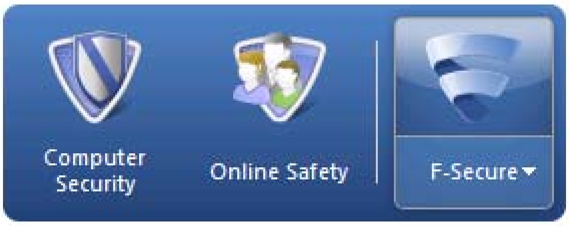
□ Computer Security

□ Online Safety

We could not find a repair function in the uninstaller, however.

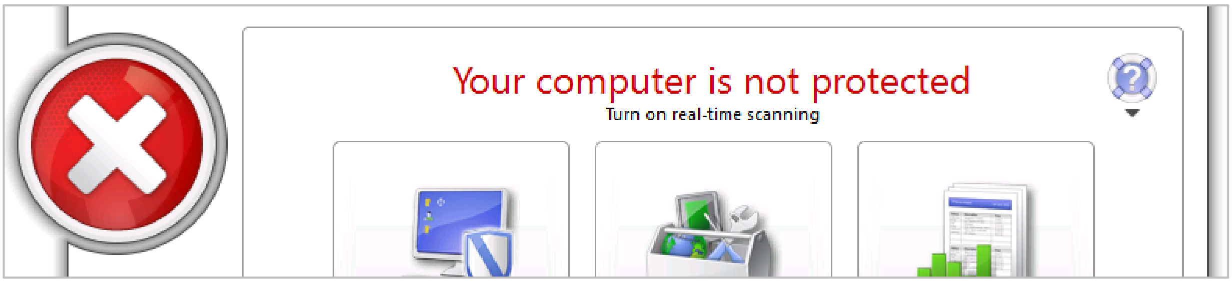
Program interface

F-Secure is very unusual in separating the components of its suite into two completely separate windows, Computer Security (antimalware and antispam) and Online Safety (parental controls). Both windows are opened by (double) clicking on the F-Secure Desktop/Start Menu icon, and then clicking on the appropriate icon on the Launcher, which appears temporarily above the Taskbar:



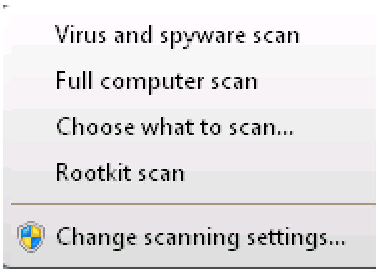
A third button on the Launcher opens the F-Secure website (top half) or displays a similar menu to the one found by right-clicking the System Tray icon. As far as we know, there is no means of creating a shortcut directly to Computer Security, or pinning it to the Taskbar; it is always necessary to go via the launcher. As noted last year, we do not understand why F-Secure have chosen to split the program into two windows and create the Launcher to start them; we suspect some users may find this irritating and/or confusing. The remainder of this report is concerned only with the Computer Security window/functions.

The layout of the main window will be familiar to users of earlier versions of the product. There are three big buttons in the middle of the window, entitled Status, Tools, and Statistics. There is a status display in the form of a circular icon in the top left-hand corner of the window, which shows a tick (checkmark) on green if all is well; there is also a text line across the top of the window, which states "Your computer is protected" if there are no problems. If real-time protection is disabled, the icon changes to a cross on red, and the text to "Your computer is not protected":



Unfortunately, F-Secure still do not provide a "Fix-All" button, so it is necessary to go into the settings and find the component that has been disabled.

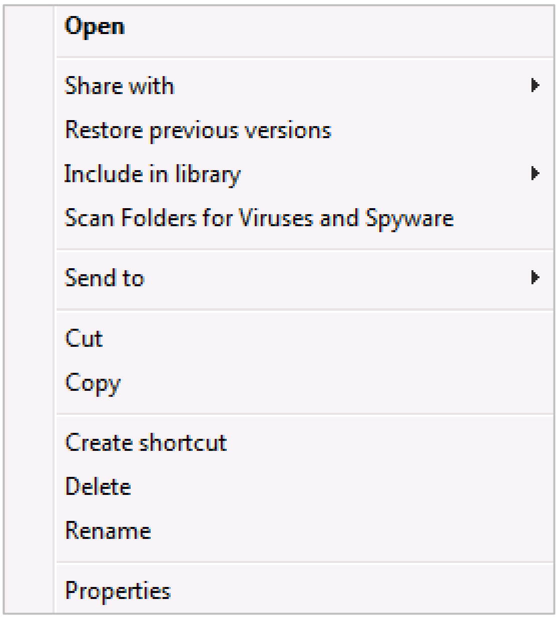
There are three smaller buttons along the bottom of the Computer Security window, namely Scan, Check For Updates, and Settings. Clicking the Scan button opens the following menu:



Whilst there is no shortage of options, we suspect that non-expert users might wonder what the difference between a "Virus and Spyware Scan" and a "Full Computer Scan" is, and indeed what a rootkit scan is, and why it needs to be done separately.

Subscription information cannot be found at all in the Computer Security window. To see how long the subscription has to run, the user has to (double) click on the F-Secure icon, click the lower part of the F-Secure button on the launcher, and then click View My Subscriptions on the resulting menu. We do not feel that we could describe this as convenient.

The local help function can be accessed from the question-mark symbol in the upper right-hand corner of the Computer Security window. F-Secure Internet Security 2013 integrates itself into Windows Explorer's context menu by means of an anonymous scan entry:



Default configuration

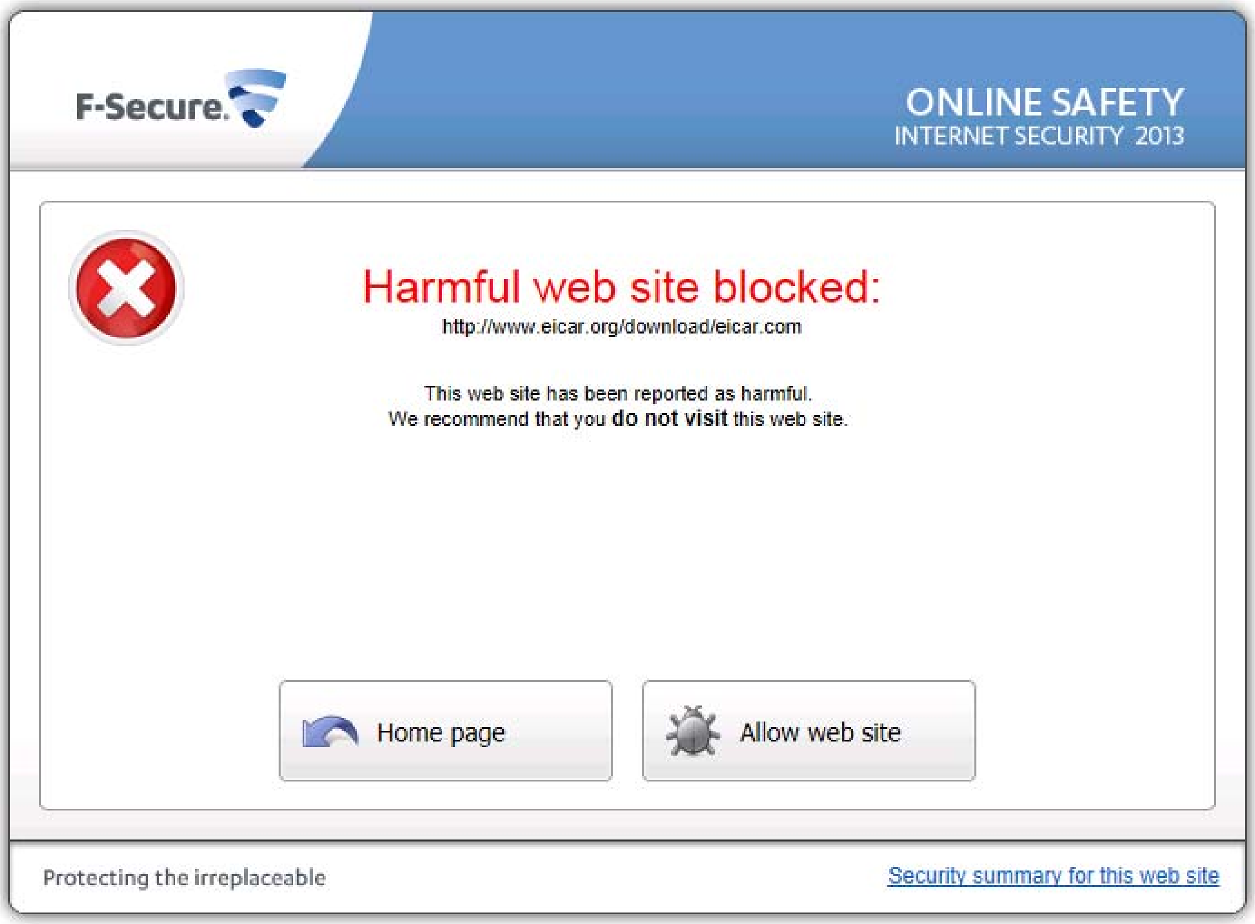
Non-administrator access

When we logged on to our test PC using a non-administrator account and clicked on the Settings button of F-Secure Computer Security, Windows displayed a User Account Control prompt demanding administrator credentials. Unless these are entered, it is impossible to disable real-time protection or change any other settings, which we find ideal.

Scanning and malware discovery

A scheduled scan is not set by default, but can easily be configured from the very obvious "Scheduled Scanning" item in the settings dialog box. We could not find a means of running a boot-time scan.

When we tried to download the EICAR test file, the page was blocked and the following dialog box displayed:



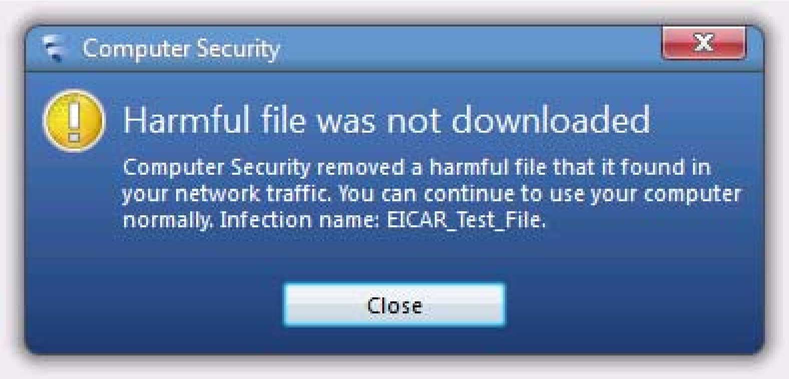
Harmful web site blocked:

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

This web site has been reported as harmful.
We recommend that you **do not visit** this web site.

Home page
Allow web site
Protecting the irreplaceable
Security summary for this web site

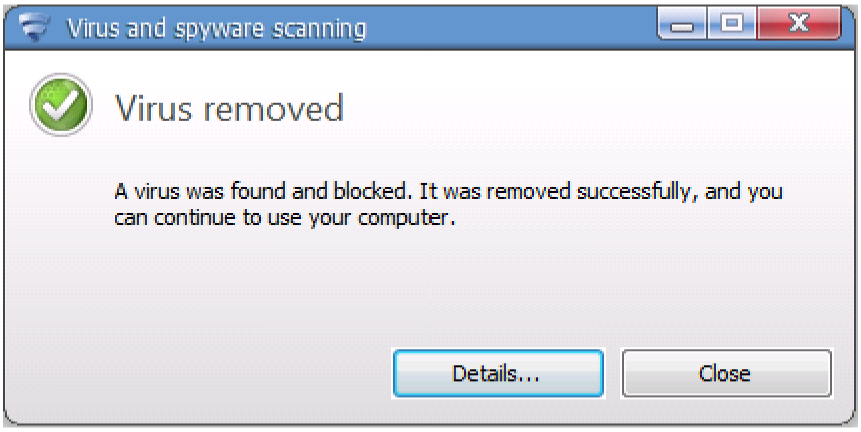
We clicked on “Allow website”, whereupon the following message box appeared:



Harmful file was not downloaded

Computer Security removed a harmful file that it found in your network traffic. You can continue to use your computer normally. Infection name: EICAR_Test_File.

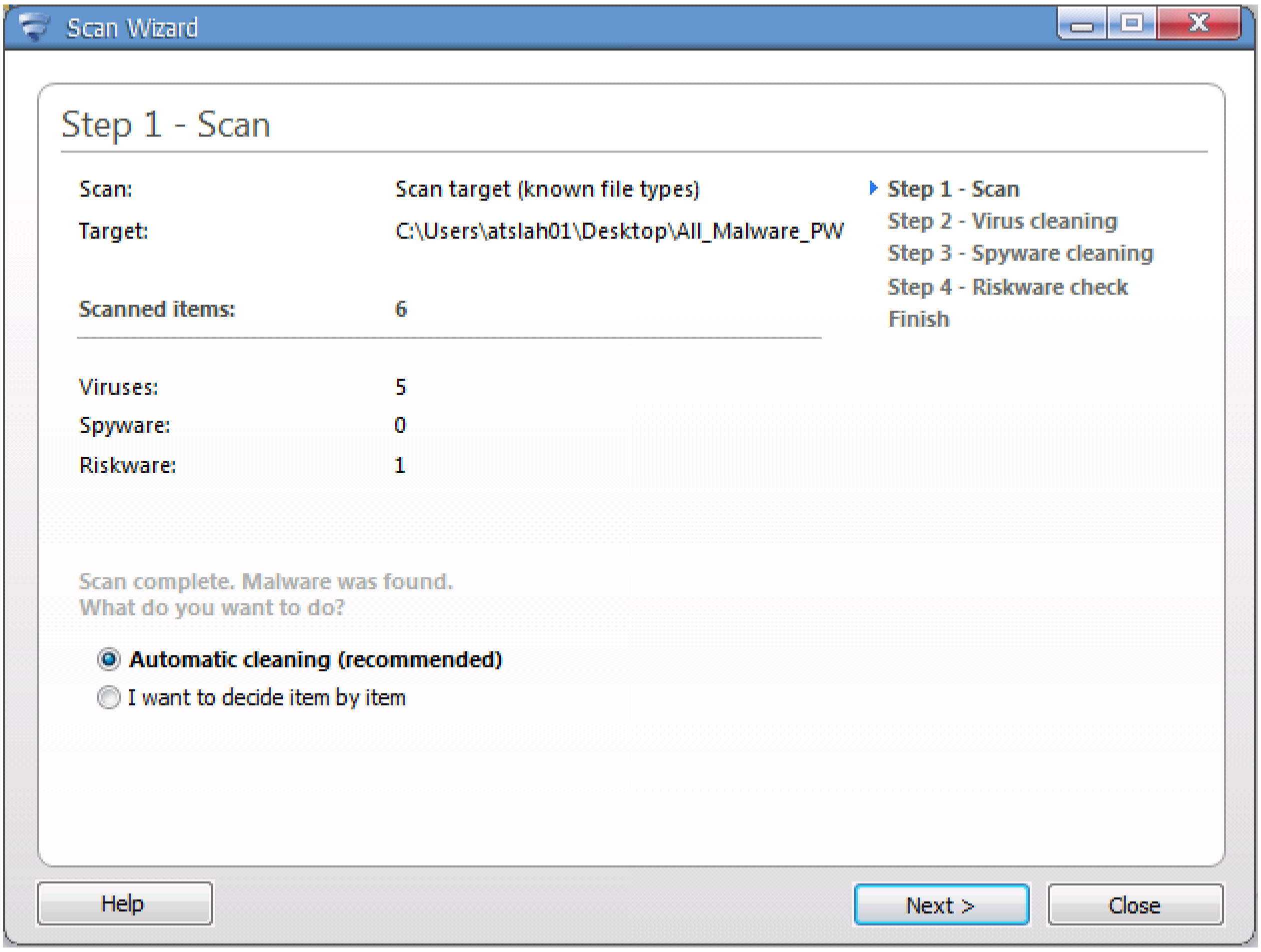
We feel this makes very clear that the computer has been protected and that the user does not need to take any action. When F-Secure's real-time protection discovered malware locally on the computer, it quarantined the items and displayed the following message:



Virus removed

A virus was found and blocked. It was removed successfully, and you can continue to use your computer.

This also makes clear that the malware has been removed and no further action is required. Advanced users can see more information about the malware by clicking Details. When we ran a custom or context-menu scan on our malware folder, F-Secure displayed the following dialog box:



Step 1 - Scan

Scan:	Scan target (known file types)
Target:	C:\Users\atslah01\Desktop\All_Malware_PW
Scanned items:	6
Viruses:	5
Spyware:	0
Riskware:	1

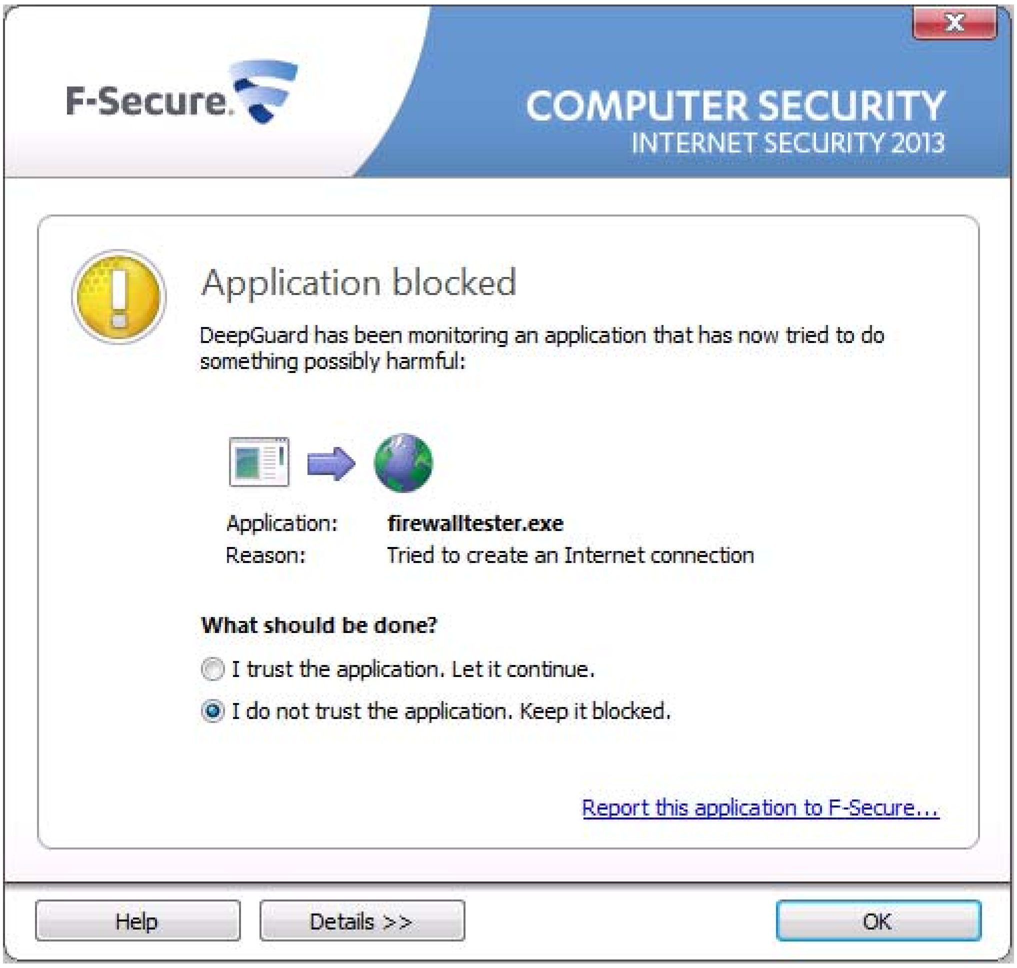
Scan complete. Malware was found.
What do you want to do?

● Automatic cleaning (recommended)
○ I want to decide item by item

This enables non-experts to remove the malware with a single click, whilst letting advanced users decide for themselves what to do.

Outbound firewall/application control

Although F-Secure Internet Security 2013 uses the Windows Firewall, it has an application control process that monitors applications attempting to connect to the Internet. When we ran our firewall testing program, F-Secure displayed the following dialog box:



Application blocked

DeepGuard has been monitoring an application that has now tried to do something possibly harmful:

Application: **firewalltester.exe**
Reason: Tried to create an Internet connection

What should be done?

○ I trust the application. Let it continue.

● I do not trust the application. Keep it blocked.

In Computer Security's settings it is possible to grant or deny permission for any individual application, or disable the monitoring of Internet access by programs altogether.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were unable to open any part of the F-Secure interface. We also found that the F-Secure scan entry was missing from the Windows Explorer context menu. Consequently, we were unable to run any sort of scan.

Help and documentation

F-Secure Internet Security 2013 has a local help service. It is a traditional-format Windows help file, with a list of topics in a narrow left hand pane, and a wider right-hand pane to display the details of the topic selected. Using the search function, we quickly and easily found clear, simple and complete instructions to both our queries. Additionally, F-Secure provides a searchable online knowledge base.

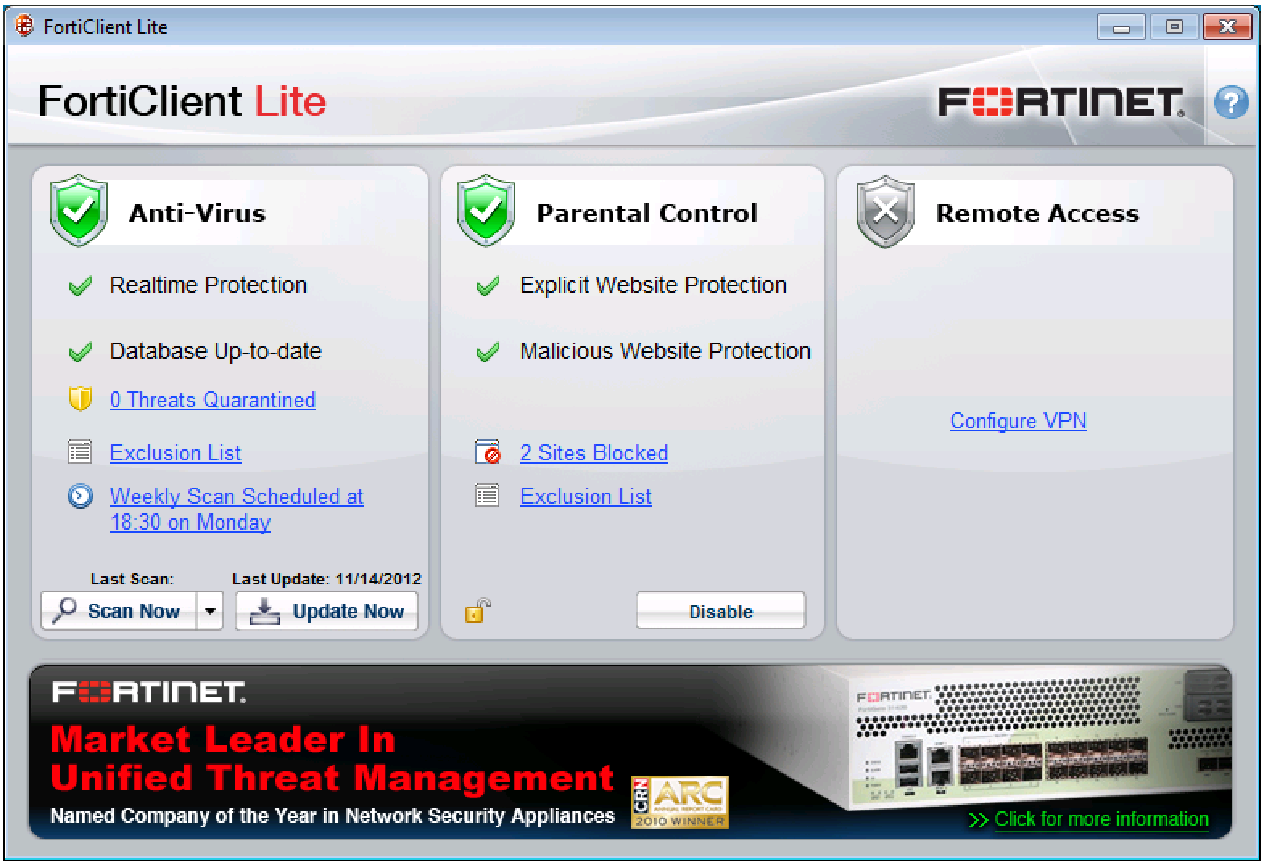
We tried searching for answers to our two standard queries, and quickly found clear and simple answers to both.

There is also a 46-page manual which can easily be downloaded from the F-Secure website. It is reasonably comprehensive, and covers installation, configuration and use of the suite. It is clearly written and laid out, has been well bookmarked, and has a detailed contents page with links to the items concerned. Its one drawback is that there are no screenshots (other than a few pictures of individual icons).

Verdict

We found F-Secure Internet Security 2013 to be largely very straightforward to use, although we question the value of the two separate windows and the Launcher. Alerts and malware notifications are excellent, although we still feel that a Fix-All button on the main program window would be very useful. Local and online help functions and the manual are very good. One significant suggestion for improvement would be to allow scanning in Safe Mode.

Fortinet FortiClient Lite 4.3.2



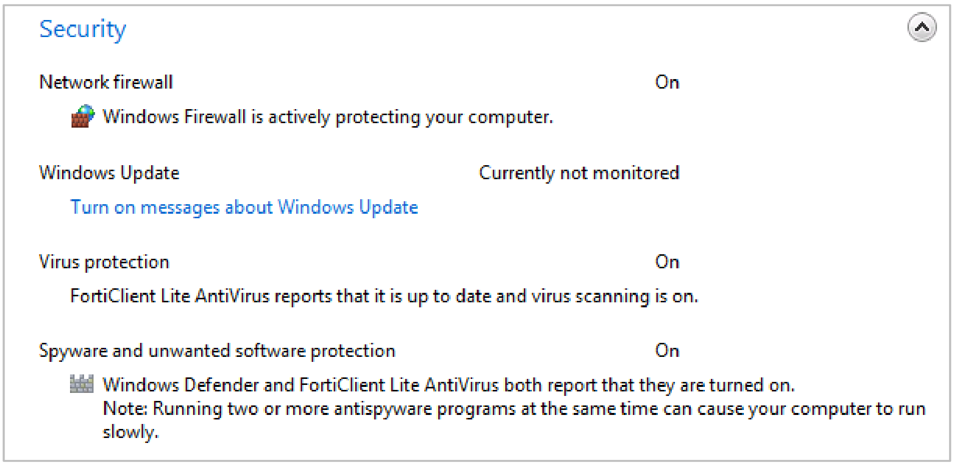
Components

FortiClient Lite is an antivirus and antispyware program. It also includes a parental control component and a VPN client.

Installation

We installed FortiClient Lite from a 253 KB downloader file. The setup wizard is very short and simple and involves just accepting the licence agreement, choosing the installation folder location, and deciding whether to use “performance optimisation”, which is claimed to improve the program’s performance when installed. A reboot was not required.

FortiClient Lite registers itself in Windows Action Center as an antivirus and antispyware program. Windows Defender is not disabled.



Security

Network firewall On

Windows Firewall is actively protecting your computer.

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

FortiClient Lite AntiVirus reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

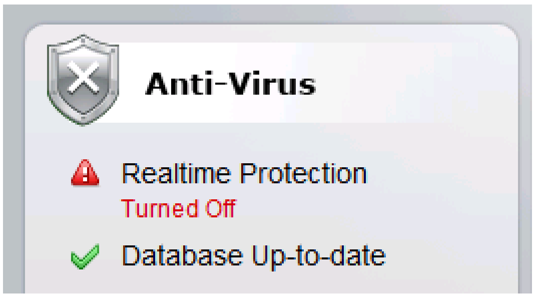
Windows Defender and FortiClient Lite AntiVirus both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

If FortiClient Lite's real-time protection is disabled, Windows Action Center immediately displays its normal alert.

The program's uninstaller has 3 options: Uninstall, Change, and Repair. Change allows the Web Filter and VPN components to be removed.

Program interface

FortiClient Lite's main program window consists of three vertical panes, entitled Anti-Virus, Parental Control, and Remote Access. The Anti-Virus column shows a shield icon next to the title, which functions as a status display. If all is well, the icon is green with a white tick (checkmark); if real-time protection is turned off, the shield turns grey and shows a cross. There are also separate status lines for the real-time protection and virus database:

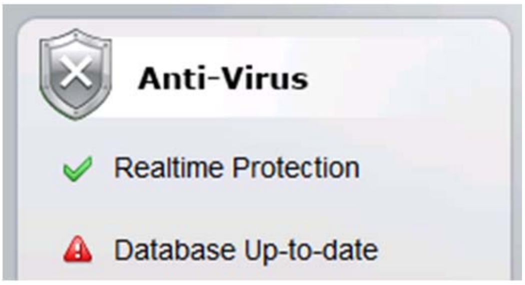


Anti-Virus

Realtime Protection
Turned Off

Database Up-to-date

We noted that immediately after installation, before a signature update had completed, the status display showed the rather confusing combination of a red warning triangle and the text "Database Up-to-date", which is easily interpreted as "Database IS up to date". We suggest that Fortinet might make the text change to "Database NOT up to date" when appropriate.



Anti-Virus

Realtime Protection

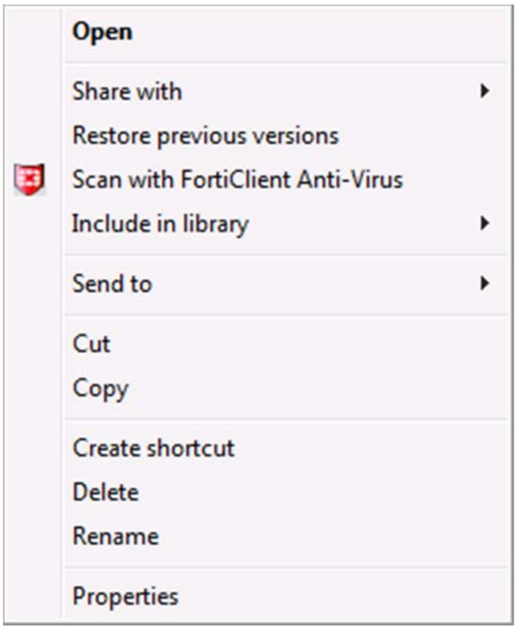
Database Up-to-date

To manually disable or enable the real-time protection, it is necessary to right-click the program's System Tray icon, and first click "Run as administrator". Right-clicking the icon again then activates the option to disable/enable the real-time protection. Whilst we see every sense in making it harder to disable the RTP, we wonder whether it might not be better to add a "Fix-all" button to the program window, allowing RTP to be reactivated with a single click if necessary.

At the bottom of the Anti-Virus section in the main program window are buttons entitled Scan Now and Update Now. The Scan Now button has a mini-menu, with the options Custom Scan, Full Scan, and Quick Scan.

There is a Help button in the top right-hand corner of the window. Clicking this opens an information box with links to the Quick Start Guide and the Fortinet website.

FortiClient Lite integrates itself into Windows Explorer's context menu with a scan entry:



As it is a free program, FortiClient Lite does not have a subscription, hence there is no need to display subscription information.

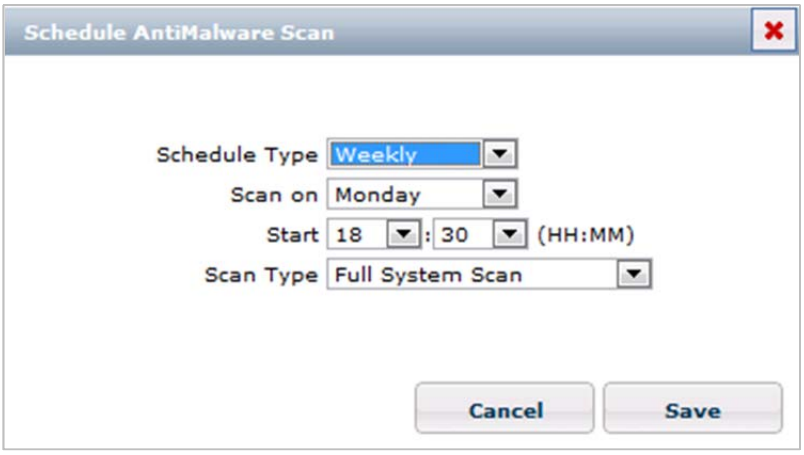
Default configuration

Non-administrator access

As mentioned above, disabling the real-time protection in FortiClient Lite requires the user to right-click the program's System Tray icon and select "Run as Administrator". When we logged on to our test PC with a non-administrator account, doing this resulted in a Windows User Account Control dialog box, which demanded administrator credentials. Unless these are entered, the RTP cannot be disabled, which we feel is ideal.

Scanning and malware discovery

FortiClient Lite sets up a scheduled scan by default. It is one of few programs to display the date and time of the next scan on its home page. Clicking on this item brings up a very simple but effective dialog box, which allows the nature and timing of the scan to be changed. We feel this is a very useful feature.



Schedule AntiMalware Scan

Schedule Type: Weekly

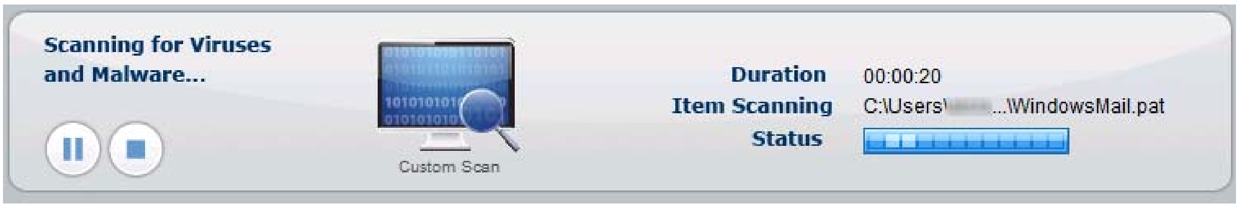
Scan on: Monday

Start: 18 : 30 (HH:MM)

Scan Type: Full System Scan

We could not find any way of performing a boot-time scan in the scan options.

We note that when a scan is run from the button in the main window, the bottom panel, which normally functions as an advertisement for Fortinet, changes to show the scan details, with controls to pause or stop it:



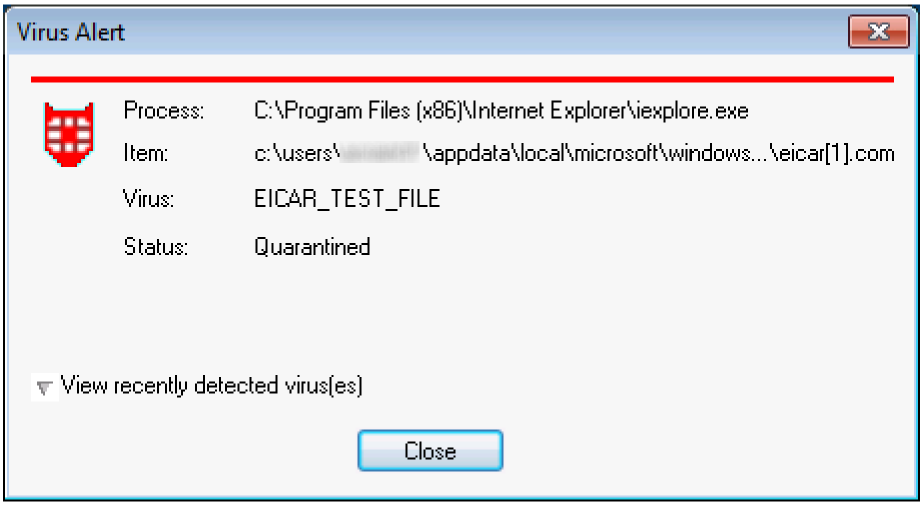
Scanning for Viruses and Malware...

Duration: 00:00:20

Item Scanning: C:\Users\[redacted]...WindowsMail.pat

Status

When we attempted to download the EICAR test file, FortiClient blocked the download and displayed the following message below, stating that the file has been quarantined:



Virus Alert

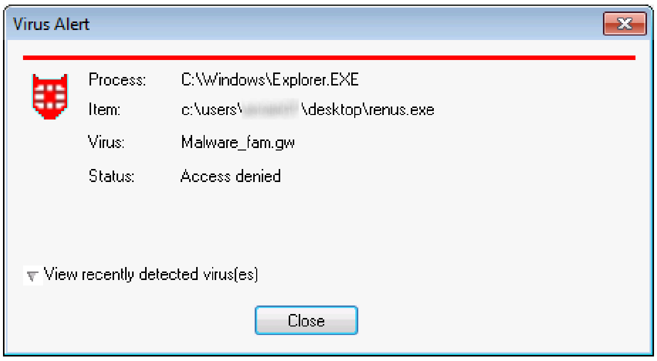
Process: C:\Program Files (x86)\Internet Explorer\iexplore.exe

Item: c:\users\[redacted]\appdata\local\microsoft\windows...\eicar[1].com

Virus: EICAR_TEST_FILE

Status: Quarantined

When the program's real-time protection found malware locally on our test PC, it showed the following message box, stating that access had been denied:



Process: C:\Windows\Explorer.EXE
Item: c:\users\[redacted]\desktop\renus.exe
Virus: Malware_fam.gw
Status: Access denied

Whilst the computer is protected and the malware cannot run, we wonder whether an option to delete or quarantine the malware might not be an improvement. When we ran a custom or context-menu scan on our malware folder, FortiClient Lite quarantined the items without prompting, and then suggested rebooting the computer to finish cleaning the PC.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were unable to use FortiClient Lite in any way. Attempting to start the program displays a message box which states "Administrator rights are required to start FortiClient Lite!"; this appears even if the program's icon is right-clicked and "Run as administrator" is selected. The context-menu entry for FortiClient does not appear in Safe Mode, so there is no way to use the program at all.

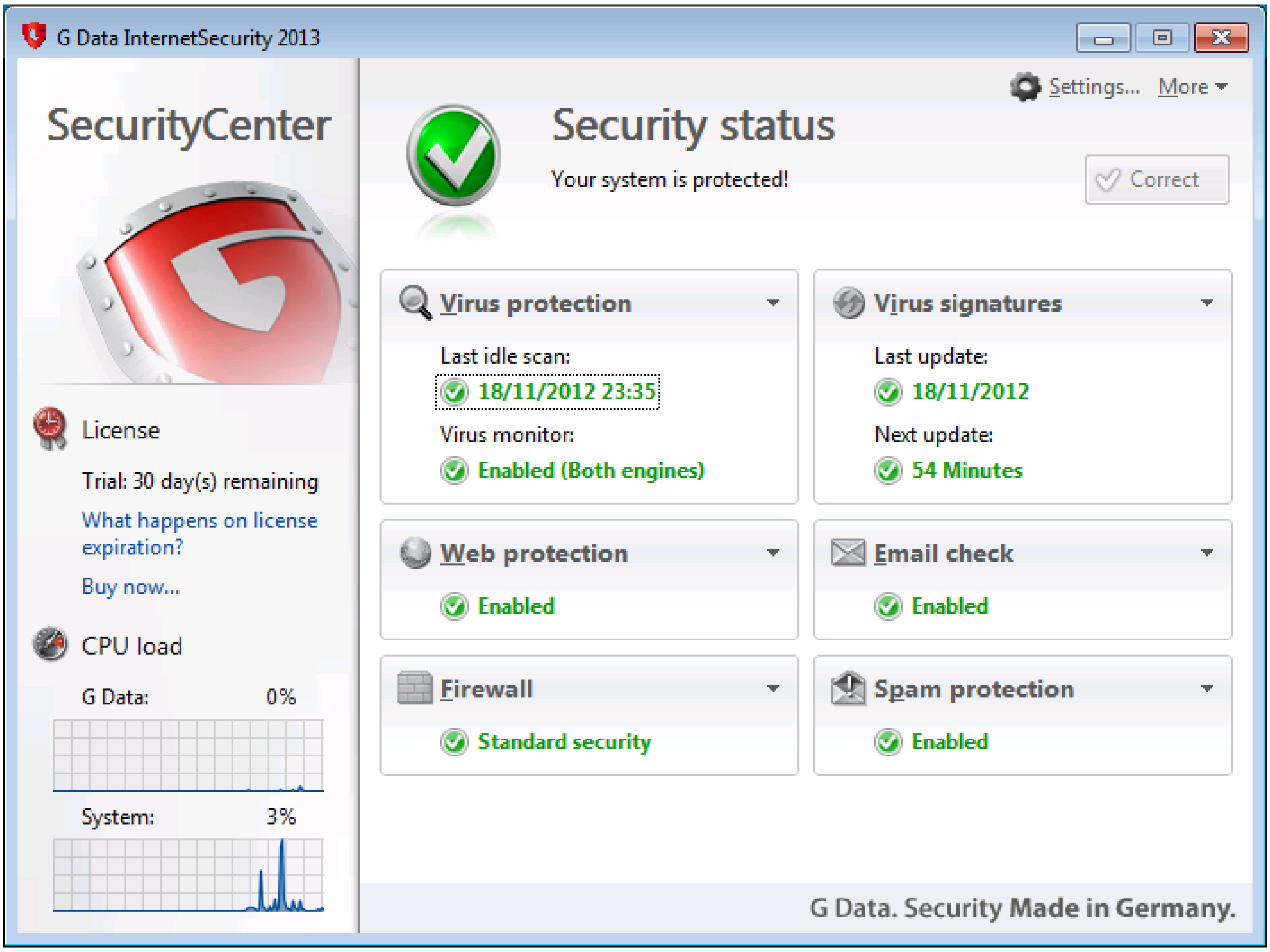
Help and documentation

There is no local Help function in FortiClient Lite, but the information box that appears when the Help icon is clicked has a link to download the Quick Start Guide. Although this document has 9 pages in total, only 2 actually contain instructions on using the program (the other 7 are cover pages and licence agreement). The text on these two pages is large enough to read comfortably at normal magnification, with the net result that the document only gives a very brief overview of the most essential functions. The manual does include links to the technical documentation and Knowledge Center pages of the Fortinet website, however. Unfortunately, we were unable to find anything on the website that might be described as a normal user guide for the program, only an administrator's guide which concentrates on issues such as automated installation is business networks. However, we note that the full FortiClient software, which is more akin to a consumer security suite, does have a comprehensive user manual. We also assume that FortiClient Lite is not intended for consumer use, which would explain the lack of documentation applicable to a home user.

Verdict

FortiClient Lite provides essential antivirus protection. Within the limitations of its scope, we found it to be well designed, making essential tasks and information easily accessible, with sensible default settings. Our one significant suggestion for improvement would be to enable some form of malware scanning in Safe Mode.

G Data Internet Security 2013



G Data InternetSecurity 2013

SecurityCenter

Security status

Your system is protected!

License

Trial: 30 day(s) remaining

What happens on license expiration?

Buy now...

CPU load

G Data: 0%

System: 3%

Virus protection

Last idle scan: 18/11/2012 23:35

Virus monitor: Enabled (Both engines)

Virus signatures

Last update: 18/11/2012

Next update: 54 Minutes

Web protection: Enabled

Email check: Enabled

Firewall: Standard security

Spam protection: Enabled

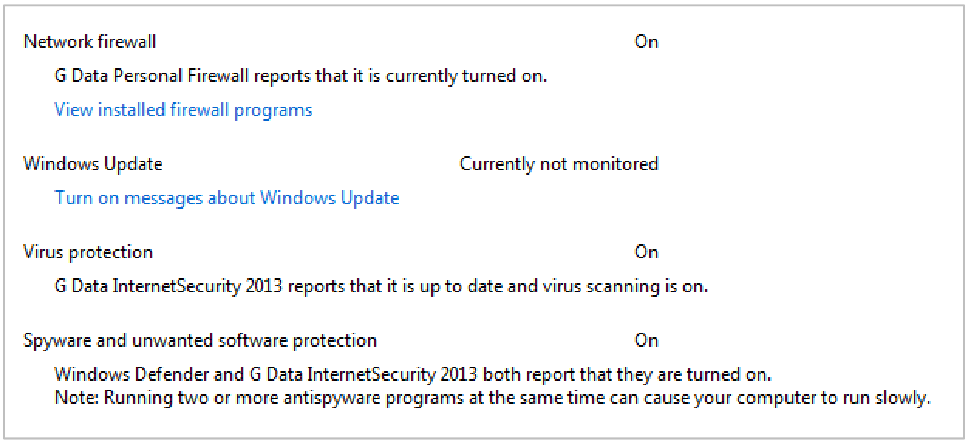
Components

G Data Internet Security 2013 comprises an antimalware component with emails scanning, antispam, firewall, parental controls, and a “shredder”, i.e. a component that securely deletes files.

Installation

We installed the trial version of G Data Internet Security, which is provided as a 629 MB full installer file. We note that the setup wizard checks for newer versions before proceeding, which we find optimal. There is a choice of major European languages, a licence agreement to accept, and an optional malware data sharing program. The user then has the choice of Complete or Custom installations; we chose the latter, which provided a complete choice of components to install. The default configuration, which we accepted, does not install the parental controls or shredder. Further options are accepting hourly updates (the default, we accepted this), and entering a licence key or using the trial version. A reboot was required at the end of the process.

G Data Internet Security 2013 registers with Windows Action Center as an antivirus and antispyware program and firewall. Windows Firewall is disabled, Windows Defender is not:



Network firewall On

G Data Personal Firewall reports that it is currently turned on.

View installed firewall programs

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

G Data InternetSecurity 2013 reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

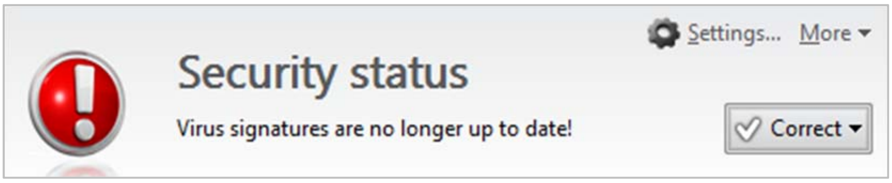
Windows Defender and G Data InternetSecurity 2013 both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

If real-time protection or the firewall is disabled, Windows Action Center produces its normal alert.

G Data's uninstaller provides a Modify option, which allows any individual component to be added to or removed from the current configuration. There is no repair option, however.

Program interface

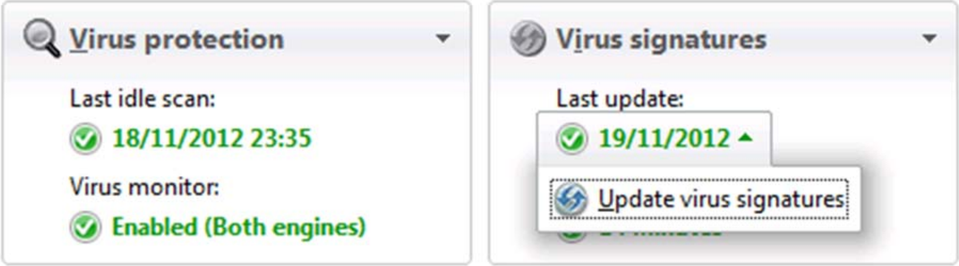
The layout of G Data Internet Security 2013's main window remains unchanged from the 2012 version. There is a main pane with a security status display at the top, and typically 6 panels displaying with controls and status information for the components installed. If a component is installed or uninstalled, its panel is added or removed accordingly. The security status section consists of text stating "Your system is protected!", and a big tick (checkmark) symbol on green, if all is well. If there is a problem, the symbol changes to an exclamation mark on red, and the text describes the exact nature of the problem, e.g. "The virus monitor has been disabled!". There is a big Correct button to the right of this text; clicking it takes measures to fix the problem:



Security status

Virus signatures are no longer up to date!

We feel that three important functions, namely updating, scanning and help, could reasonably be described as “slightly hidden”. The green status display text in each of the panels functions as a mini-menu; the scan menu can be found by clicking on the date of the last idle scan in the Virus Protection panel, and the signatures can be updated by clicking on the date of the last update, as shown below:



Virus protection

Last idle scan: 18/11/2012 23:35

Virus monitor: Enabled (Both engines)

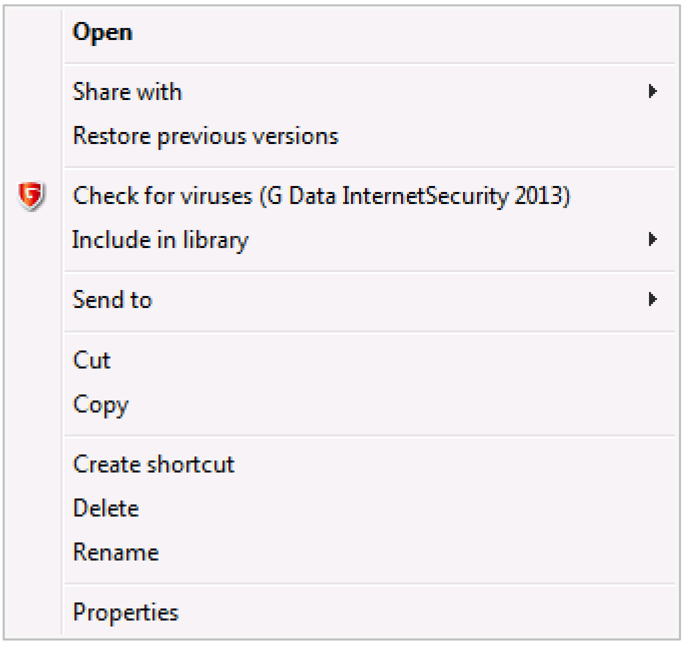
Virus signatures

Last update: 19/11/2012

The help function can be found in the More menu in the top right-hand corner of the window. Whilst an advanced user would easily find all three of these functions very quickly with a little exploration, we wonder whether non-experts might prefer to see three buttons marked Scan, Update, Help, directly on the home page.

Subscription information is clearly displayed in the panel on the left-hand side of the window.

G Data adds its own scan entry to the Windows Explorer context menu:



Default configuration

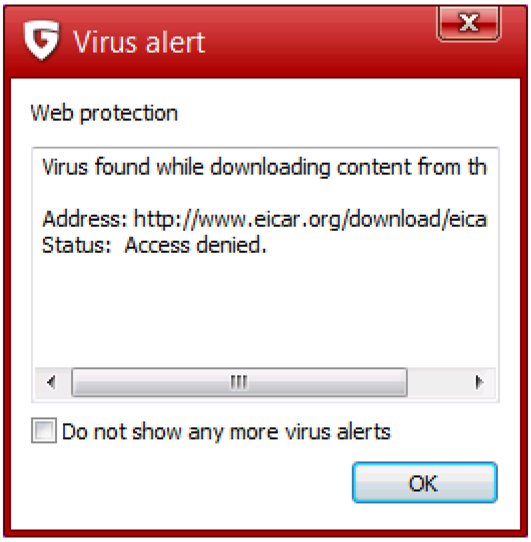
Non-administrator access

When we logged on to our test PC with a non-administrator account, attempting to disable the real-time protection produced a Windows User Account Control prompt, which demanded administrator credentials. Unless these are entered, the protection cannot be disabled, which we find optimal.

Scanning and malware discovery

A scheduled scan is not activated by default, although the Idle Scan (which scans the computer when it is not being used) is. A scheduled scan can easily be configured from the Automatic Virus Checks settings dialog. We could not find a means of running a boot-time scan from the program, although the G Data installation CD can be used for this purpose. There is a link in Windows 7's Start Menu for creating a rescue disk, which does the same.

When we attempted to download the EICAR test file, G Data blocked the web page and the download, and displayed the following alert:

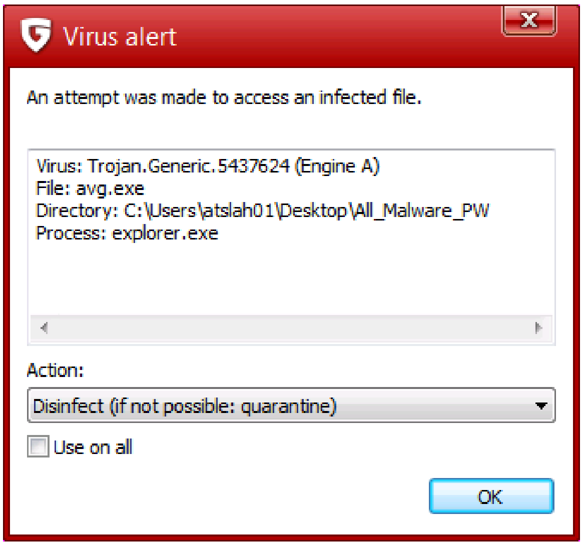


Virus found while downloading content from th

Address: http://www.eicar.org/download/eica
Status: Access denied.

Whilst the message states "Access denied", we feel the alert box could be a little clearer, especially as some of the text goes off the page and needs a scroll bar to be seen.

When malware was discovered locally on the PC by G Data's real-time protection, the following alert was shown:



Virus alert

An attempt was made to access an infected file.

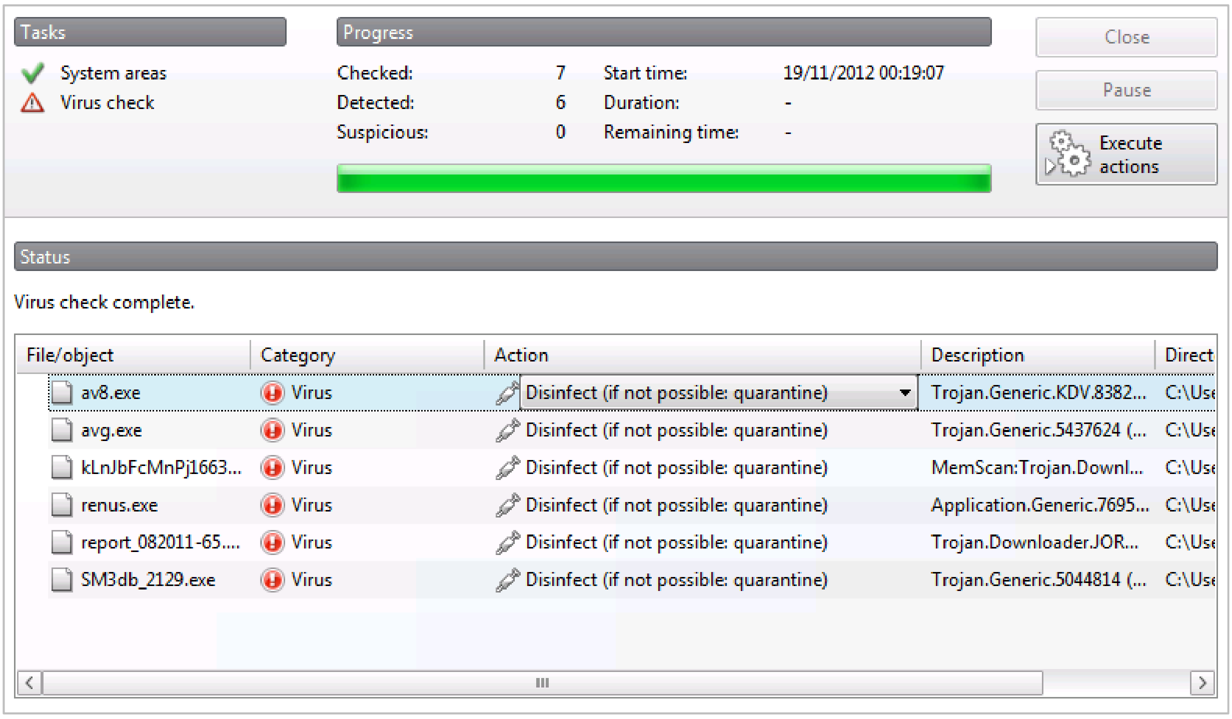
Virus: Trojan.Generic.5437624 (Engine A)
File: avg.exe
Directory: C:\Users\atslah01\Desktop\All_Malware_PW
Process: explorer.exe

Action:
Disinfect (if not possible: quarantine)

□ Use on all

The default action, "Disinfect (if not possible, quarantine)", will remove all harmful code from a file and thus prevent any infection. In the event that the file discovered is an actual virus (malicious code within a benign file), this action is ideal; however, with a more common Trojan, it leaves behind a 0 KB file, which may be a little confusing to non-experts.

When we scanned our malware folder from the G Data console or context menu, the following dialog box was shown:



Tasks

✓ System areas
⚠ Virus check

Progress

Checked:	7	Start time:	19/11/2012 00:19:07
Detected:	6	Duration:	-
Suspicious:	0	Remaining time:	-

Status

Virus check complete.

File/object	Category	Action	Description	Direct
av8.exe	Virus	Disinfect (if not possible: quarantine)	Trojan.Generic.KDV.8382...	C:\Use
avg.exe	Virus	Disinfect (if not possible: quarantine)	Trojan.Generic.5437624 (...	C:\Use
kLnJbFcMnPj1663...	Virus	Disinfect (if not possible: quarantine)	MemScan:Trojan.Downl...	C:\Use
renus.exe	Virus	Disinfect (if not possible: quarantine)	Application.Generic.7695...	C:\Use
report_082011-65....	Virus	Disinfect (if not possible: quarantine)	Trojan.Downloader.JOR...	C:\Use
SM3db_2129.exe	Virus	Disinfect (if not possible: quarantine)	Trojan.Generic.5044814 (...	C:\Use

This enables all items to be processed using the same default action with a single click, which is very easy for non-experts. Alternatively, advanced users can set a different action for individual files if they so choose.

Inbound firewall settings

When we installed G Data Internet Security 2013 on our test PC, it did not prompt us for the network type (public or private) for the existing network. We found that after installation, we were able to access the PC's file share, ping it, and connect via Remote Desktop, just as we had before. Changing the network type from Work to Public in Windows Network and Sharing Center made no difference to this access.

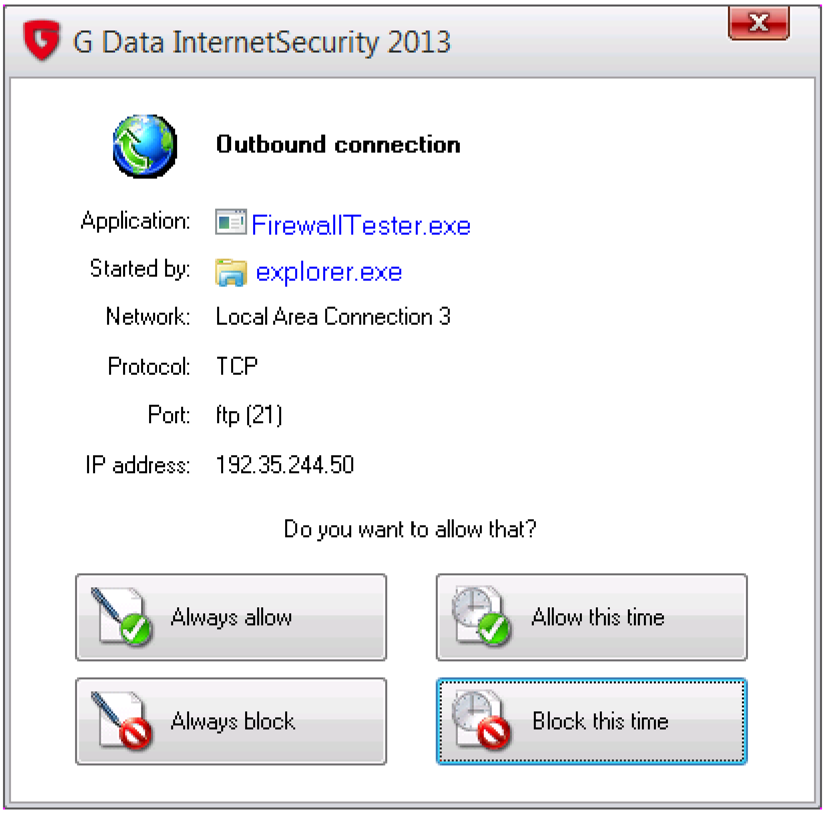
When we connected our test PC to a new network, which we defined as Public in Windows Network and Sharing prompt, there was no further query from G Data as to the network type. We found that we could not access the test PC's file share from another PC on the new network, but that we could successfully ping it (both IPv4 and IPv6) and access it by Remote Desktop. Only when we manually changed the network type in G Data's own settings to "Direct Internet Connection" were all forms of access closed off. We feel that this could easily result in users connecting to public wireless networks, selecting Public in the Windows prompt, and incorrectly assuming that all access to their computer from the network was blocked. We would urge G Data to rectify this.

Outbound firewall/application control

When we ran our firewall testing program, it failed to complete its task, without any notification from G Data. We investigated, and found that it had been silently blocked by G Data's Application Radar (application control) component. We feel that this is a better default action than asking the user whether to allow a program to run or not; however, some users might like to see a notification stating that G Data had blocked the program.

We were able to allow the firewall tester in the settings; having done this, we found that it completed its task without any query or hindrance when run again.

Switching off the Autopilot mode (automatic decision-making by the firewall/application control) produced the following dialog when we next ran the firewall tester:



G Data InternetSecurity 2013

Outbound connection

Application: FirewallTester.exe
Started by: explorer.exe
Network: Local Area Connection 3
Protocol: TCP
Port: ftp (21)
IP address: 192.35.244.50

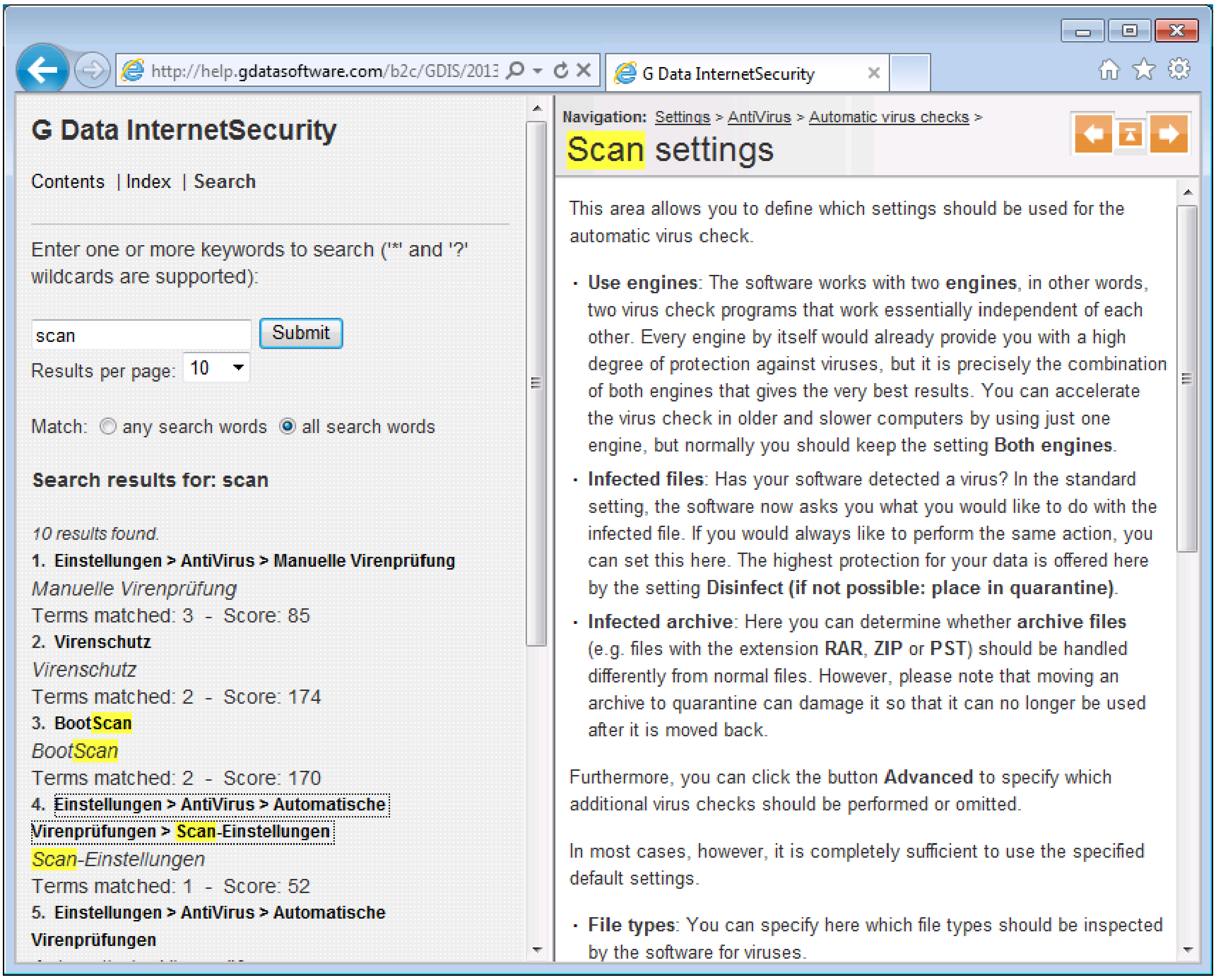
Do you want to allow that?

Safe Mode

We were unable to run any kind of scan with G Data Internet Security when we started our PC in Safe Mode with Networking.

Help and documentation

The Help entry in the “More” menu opens the online help service on G Data’s website. This is arranged much like a Windows Help file, with a left-hand column showing common topics, with a bigger right-hand panel to display details of the item chosen. There is also an index and search function. Searching for our two test items, scheduled scan and scan exceptions, drew a complete blank, with no results found however we phrased the queries. Perplexed that an apparently comprehensive search function should fail to find any results for these topics, we tried searching simply for “scan”. We were astonished to see that this produced a wide variety of answers in the left-hand pane *in German*:



G Data InternetSecurity

Contents | Index | Search

Enter one or more keywords to search ('*' and '?' wildcards are supported):

scan Submit

Results per page: 10

Match: ○ any search words ● all search words

Search results for: scan

10 results found.

1. **Einstellungen > AntiVirus > Manuelle Virenprüfung**
Manuelle Virenprüfung
Terms matched: 3 - Score: 85
2. **Virenschutz**
Virenschutz
Terms matched: 2 - Score: 174
3. **BootScan**
BootScan
Terms matched: 2 - Score: 170
4. **Einstellungen > AntiVirus > Automatische Virenprüfungen > Scan-Einstellungen**
Scan-Einstellungen
Terms matched: 1 - Score: 52
5. **Einstellungen > AntiVirus > Automatische Virenprüfungen**

Navigation: Settings > AntiVirus > Automatic virus checks >

Scan settings

This area allows you to define which settings should be used for the automatic virus check.

- **Use engines**: The software works with two **engines**, in other words, two virus check programs that work essentially independent of each other. Every engine by itself would already provide you with a high degree of protection against viruses, but it is precisely the combination of both engines that gives the very best results. You can accelerate the virus check in older and slower computers by using just one engine, but normally you should keep the setting **Both engines**.
- **Infected files**: Has your software detected a virus? In the standard setting, the software now asks you what you would like to do with the infected file. If you would always like to perform the same action, you can set this here. The highest protection for your data is offered here by the setting **Disinfect (if not possible: place in quarantine)**.
- **Infected archive**: Here you can determine whether **archive files** (e.g. files with the extension **RAR**, **ZIP** or **PST**) should be handled differently from normal files. However, please note that moving an archive to quarantine can damage it so that it can no longer be used after it is moved back.

Furthermore, you can click the button **Advanced** to specify which additional virus checks should be performed or omitted.

In most cases, however, it is completely sufficient to use the specified default settings.

- **File types**: You can specify here which file types should be inspected by the software for viruses.

As German speakers, we were able to understand the topic headings, and clicking on any one of them produced the correct instructions for the respective subject, in English. It happens that the word “scan” is used in German to mean the same thing as in English, in the context of antivirus programs. Essentially, the search function only works if German words are entered; thus “Settings” draws a blank, but its German translation “Einstellungen” finds a variety of answers. Needless to say, we do not think that anyone who doesn’t speak German will find this acceptable.

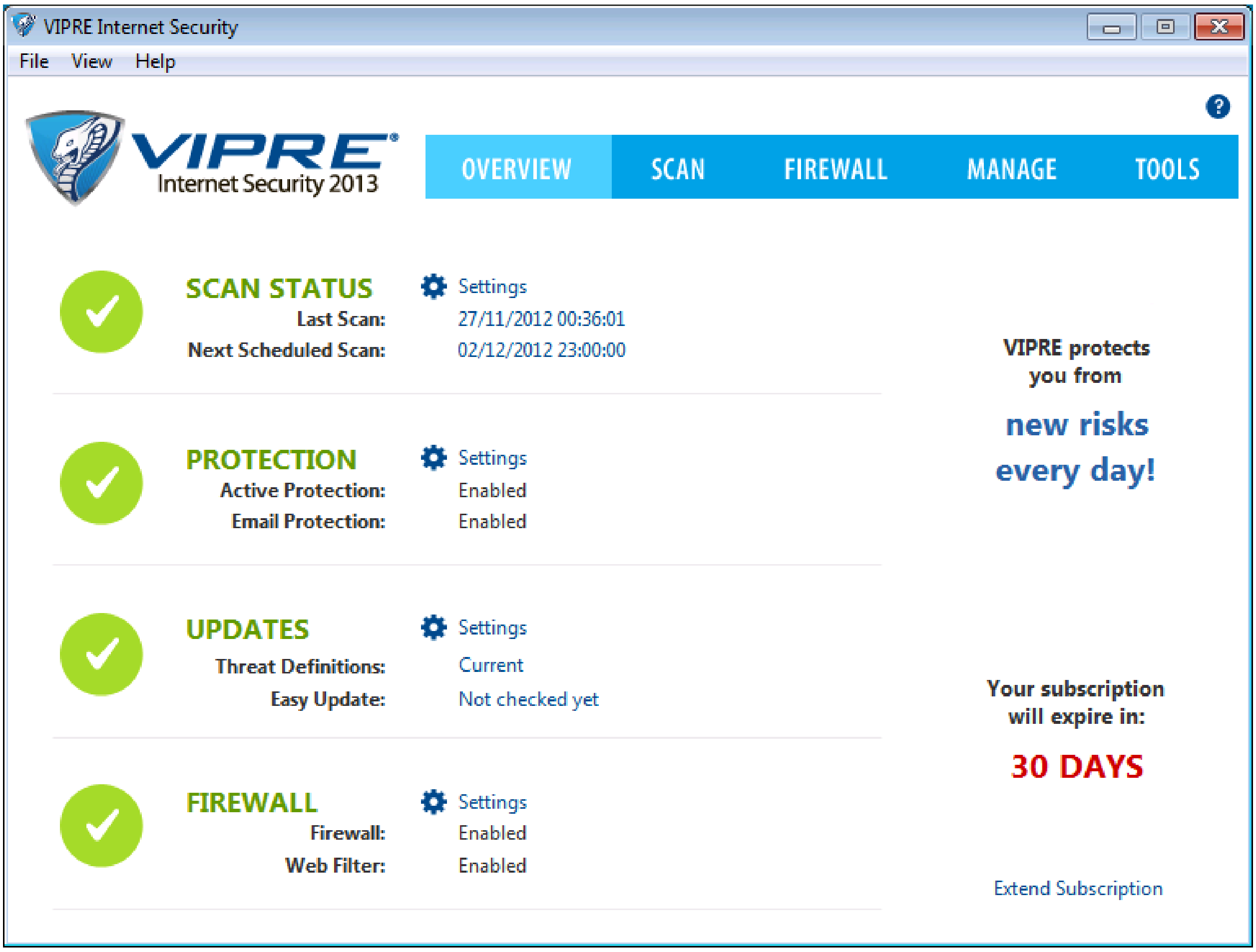
We note that we downloaded the installation file from the International website (in English), chose English as the program language during setup, and installed it on an English version of Windows, on a computer physically located in the UK, with UK English regional settings throughout.

We must also add that whilst the answers to the queries gave clear instructions as to how to use particular pages/dialog boxes within the settings, they do not appear to explain how to get to that page/dialog in the first place. We were unable to find a manual for G Data Internet Security 2013 on the manufacturer's international or US websites. In summary, we can only describe G Data's help function as disappointing.

Verdict

We found much to like in G Data Internet Security 2013's program interface. We feel the main window provides an excellent status display, both overall and in detail, and confident users should find all important information and functions easily accessible. Alerts and default actions on malware discovery seem very sensible. Unfortunately, we have to point out that joining a public network and registering this as Public in Windows' prompt does not change the settings of the G Data firewall appropriately, which we feel could leave users unprotected but unaware. We also feel that the help function could be much improved, principally by translating it fully into English for the English version.

GFI VIPRE Internet Security 2013



SCAN STATUS ⚙ Settings
Last Scan: 27/11/2012 00:36:01
Next Scheduled Scan: 02/12/2012 23:00:00

PROTECTION ⚙ Settings
Active Protection: Enabled
Email Protection: Enabled

UPDATES ⚙ Settings
Threat Definitions: Current
Easy Update: Not checked yet

FIREWALL ⚙ Settings
Firewall: Enabled
Web Filter: Enabled

VIPRE protects you from new risks every day!

Your subscription will expire in: 30 DAYS

Extend Subscription

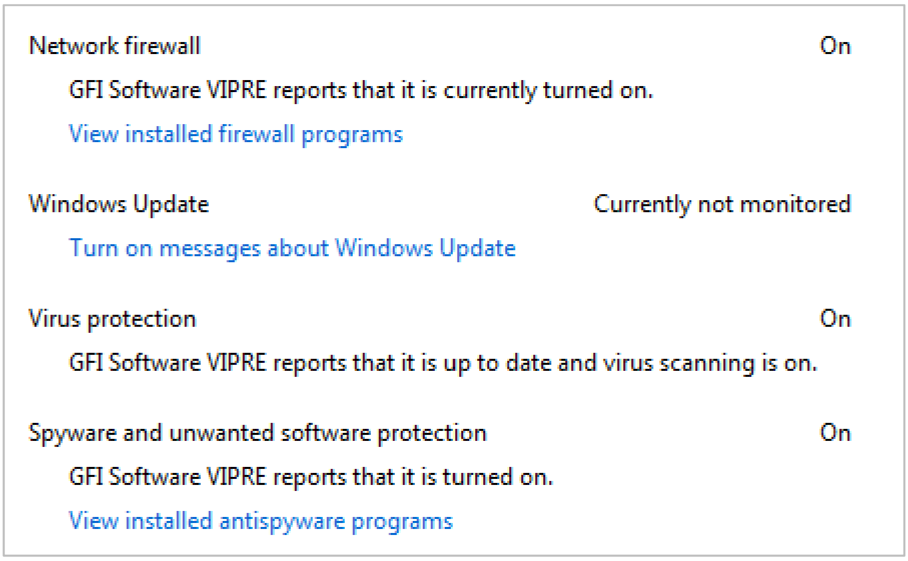
Components

VIPRE Internet Security 2013 includes antivirus and antispyware protection with email scanning, antispam, a firewall, and a shredder (secure file deletion).

Installation

The trial version of VIPRE Internet Security 2013 is installed from an 8 MB downloader file. The only option offered is to change the installation folder. Installation then proceeds and completes without any further interaction being required. A restart is needed at the end of the process. After logging on again, we were greeted by a VIPRE dialog box, which enquired whether we wanted to join the malware data sharing scheme.

VIPRE Internet Security registers with Windows Action Center as an antivirus and antispyware program and firewall. Both Windows Firewall and Windows Defender are disabled:



Network firewall On

GFI Software VIPRE reports that it is currently turned on.

View installed firewall programs

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

GFI Software VIPRE reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

GFI Software VIPRE reports that it is turned on.

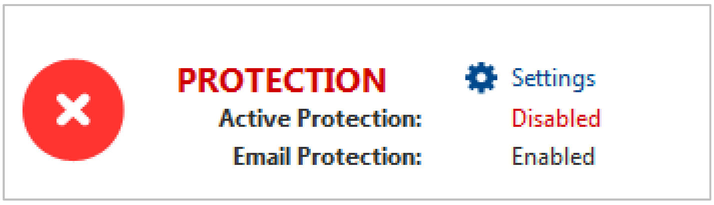
View installed antispyware programs

If real-time protection is disabled, Action Center displays its normal warning.

VIPRE's uninstaller program offers a repair function, as well as complete removal.

Program interface

The home page of VIPRE Internet Security 2013 is made up of four horizontal stripes, each one representing a status display for a component or function. These are Scan Status, Protection (meaning real-time protection), Updates and Firewall. Each has a status icon, which is a tick (checkmark) in a green circle if all is well, a Settings button, and two detailed status lines. There is no overall status display or Fix-All button, but if a major component such as real-time protection is disabled, its name and symbol turn red; clicking on the symbol, which now displays a cross, opens the relevant settings dialog box to reactivate the component.



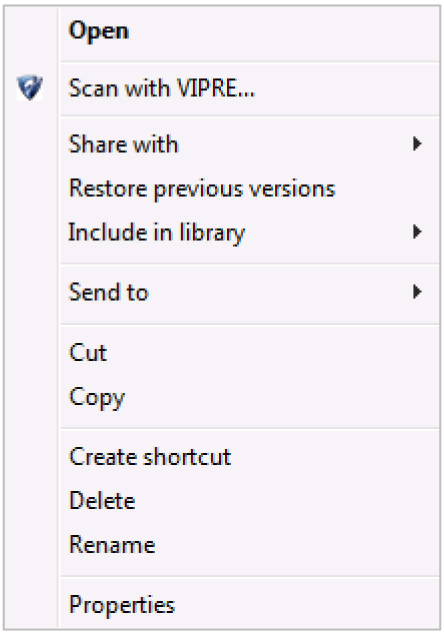
PROTECTION

Settings

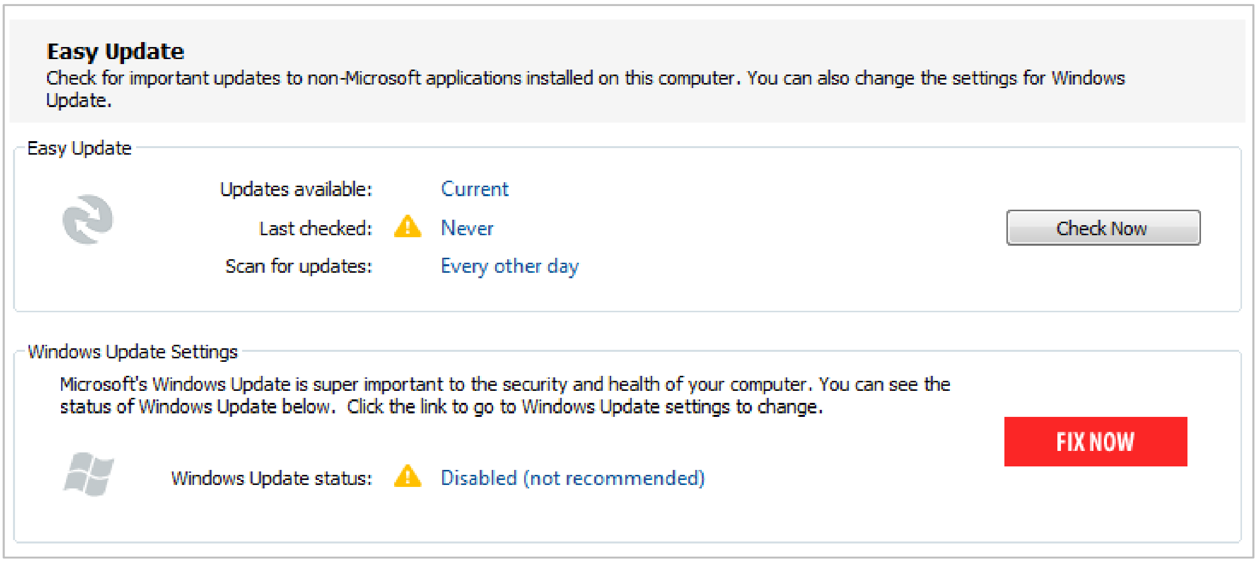
Active Protection: Disabled

Email Protection: Enabled

The status button for Updates serves as an Update Now button, to download the latest signatures. Likewise, the Scan Status button opens the scan options dialog box, which offers a Quick Scan, Deep Scan (full scan), and Custom Scan. Subscription information is very clearly displayed in the bottom right-hand corner of the window. The local help function can be opened by clicking the question-mark symbol in the top right-hand corner of the window. There is also a Help menu, which includes a link to VIPRE's online support page. VIPRE integrates itself into Windows Explorer's context menu with a scan entry:



Finally, we note that the Easy Update function displayed on the home page is in fact a vulnerability scanner, which checks the status of Windows Update and checks for newer versions of non-Microsoft programs too:



Easy Update

Check for important updates to non-Microsoft applications installed on this computer. You can also change the settings for Windows Update.

Easy Update

Updates available: Current

Last checked: ⚠ Never

Scan for updates: Every other day

Windows Update Settings

Microsoft's Windows Update is super important to the security and health of your computer. You can see the status of Windows Update below. Click the link to go to Windows Update settings to change.

Windows Update status: ⚠ Disabled (not recommended)

We regard this as an excellent feature, but feel that its name is confusing, and that some users may not realise what it is unless they actually click on it. We suggest that VIPRE might like to find a more descriptive name, such as "Windows and program updates".

Default configuration

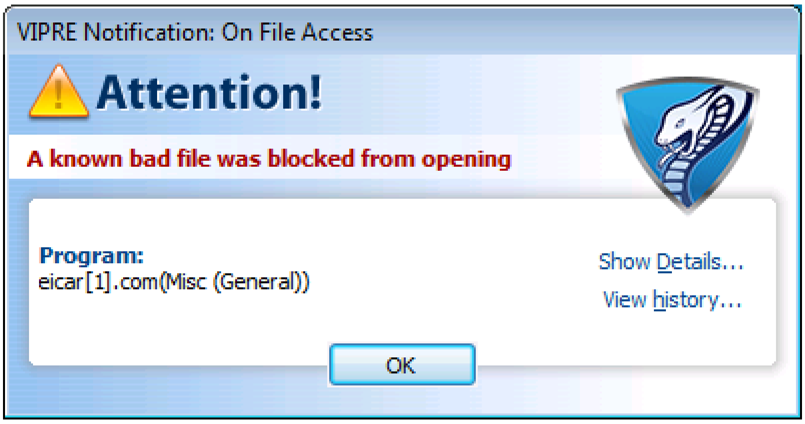
Non-administrator access

When we logged on to our test PC using a non-administrator account, we were able to deactivate real-time protection without any hindrance. We do not regard this as ideal.

Scanning and malware discovery

A scheduled scan is configured by default. It can easily be changed by clicking on the date displayed for Next Scheduled Scan on the Overview (home) page of the window. We could not find a means of running a boot-time scan.

When we tried to download the EICAR test file, VIPRE blocked the download and displayed the following alert:



VIPRE Notification: On File Access

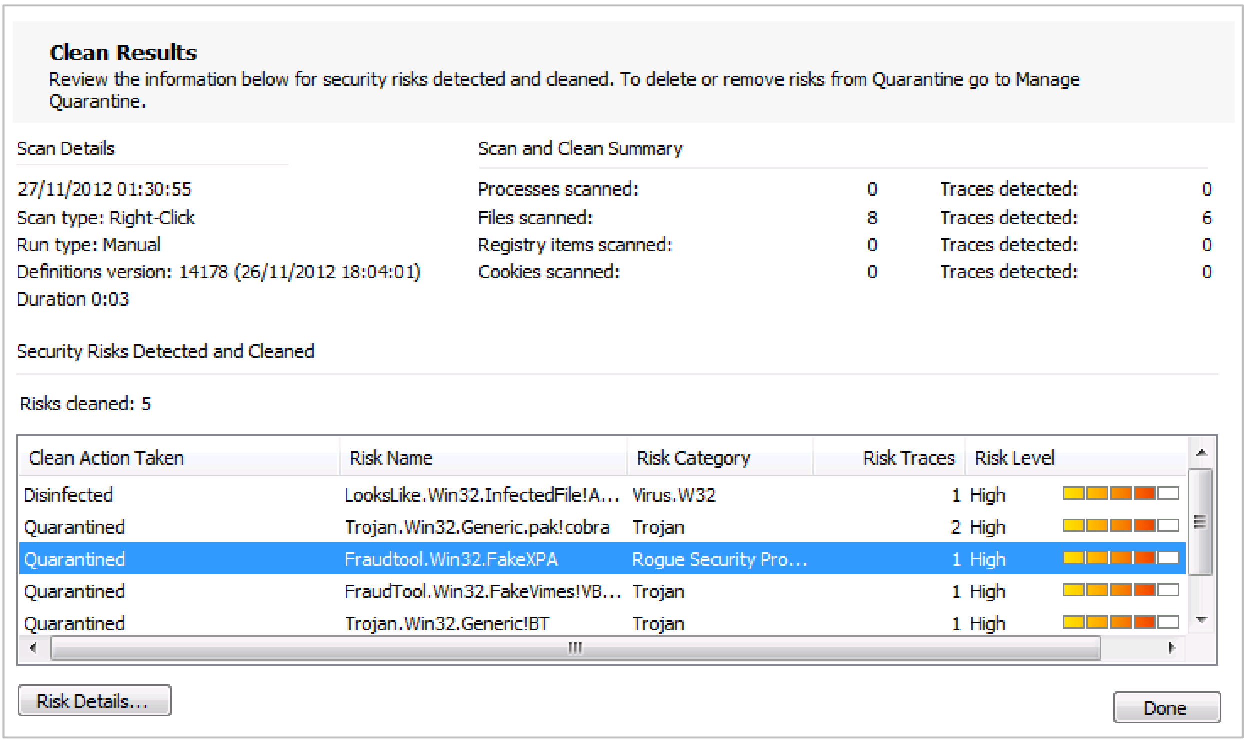
Attention!

A known bad file was blocked from opening

Program:
eicar[1].com(Misc (General))

We feel this makes reasonably clear that the “threat” has been stopped. An identical message box was shown when VIPRE’s real-time protection detected malware locally on our PC, and the malware was quarantined. A further message box recommended rebooting the PC.

When we ran a custom or context-menu scan on our folder of malware, VIPRE removed all the items automatically, and displayed the following summary:



Clean Results

Review the information below for security risks detected and cleaned. To delete or remove risks from Quarantine go to Manage Quarantine.

Scan Details

27/11/2012 01:30:55
Scan type: Right-Click
Run type: Manual
Definitions version: 14178 (26/11/2012 18:04:01)
Duration 0:03

Scan and Clean Summary

Processes scanned:	0	Traces detected:	0
Files scanned:	8	Traces detected:	6
Registry items scanned:	0	Traces detected:	0
Cookies scanned:	0	Traces detected:	0

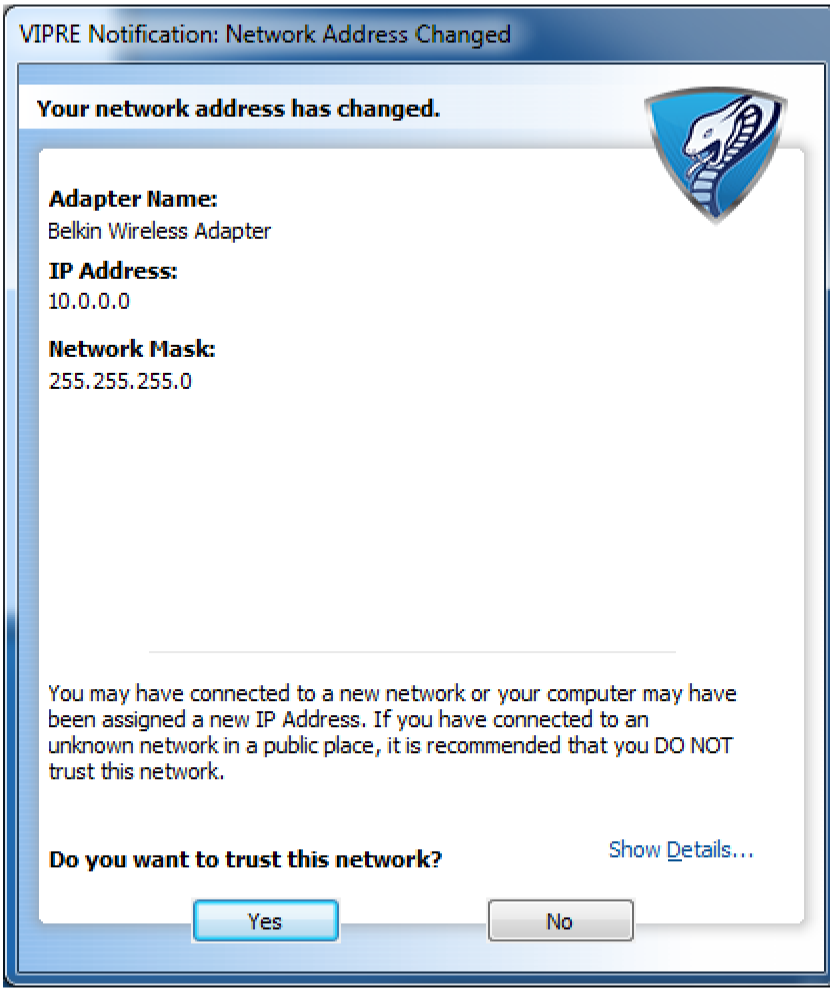
Security Risks Detected and Cleaned

Risks cleaned: 5

Clean Action Taken	Risk Name	Risk Category	Risk Traces	Risk Level
Disinfected	LooksLike.Win32.InfectedFile!A...	Virus.W32	1	High
Quarantined	Trojan.Win32.Generic.pak!cobra	Trojan	2	High
Quarantined	Fraudtool.Win32.FakeXPA	Rogue Security Pro...	1	High
Quarantined	FraudTool.Win32.FakeVimes!VB...	Trojan	1	High
Quarantined	Trojan.Win32.Generic!BT	Trojan	1	High

Inbound firewall settings

After installing VIPRE Internet Security 2013, we were able to access the PC's file share, ping it, and log on by Remote Desktop, just as before. Changing the network type to Public in Windows Network and Sharing Center had no effect, all three types of access continued to be available. When we connected our test PC to a new network, which we designated as public in the Windows Network and Sharing prompt, VIPRE displayed its own prompt, asking whether the network should be trusted:



VIPRE Notification: Network Address Changed

Your network address has changed.

Adapter Name:
Belkin Wireless Adapter

IP Address:
10.0.0.0

Network Mask:
255.255.255.0

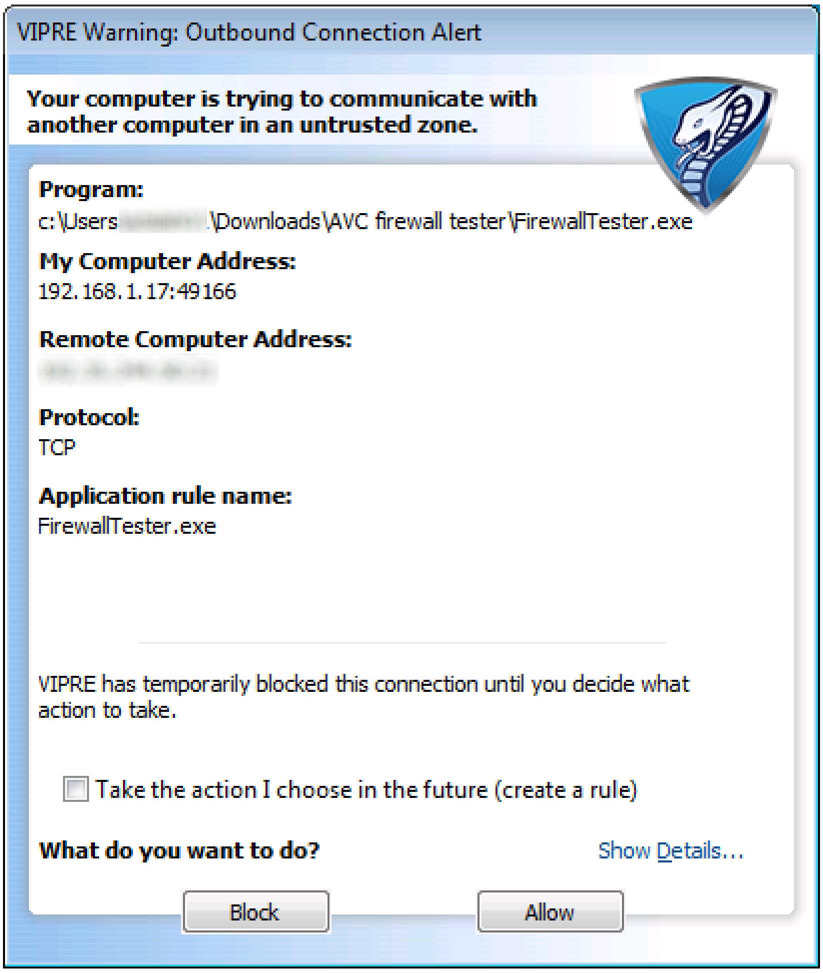
You may have connected to a new network or your computer may have been assigned a new IP Address. If you have connected to an unknown network in a public place, it is recommended that you DO NOT trust this network.

Do you want to trust this network?

We clicked No, the equivalent of designating the network as Public in Windows terminology. We then tried pinging the test PC, accessing its file share, and logging on via Remote Desktop, from another PC on the new network. We found that we were able to ping the test PC with IPv6, access the file share and edit a document in it, and log on using Remote Desktop if the hostname was specified. Pinging with IPv4 and Remote Desktop access using the IPv4 IP address failed, however. We conclude that VIPRE's firewall only blocks IPv4 traffic and allows all IPv6 traffic through. Given that Windows Vista, Windows 7 and Windows 8 all have IPv6 installed and enabled by default, there is a high chance that most of the laptop users who connect to the Internet via WLAN in a café or hotel will have IPv6 connectivity. We feel that a firewall that only blocks IPv4 traffic is thus entirely inadequate in this day and age, and urge VIPRE to implement IPv6 protection in their firewall as soon as possible.

Outbound firewall/application control

When we ran our firewall testing program, we found that it completed its task without any hindrance or alerts. By going into the Exceptions dialog of the Firewall settings, we were able to specify that VIPRE Internet Security should prompt for permission before allowing this particular program Internet access. When we ran the firewall tester again, VIPRE displayed the following prompt:



VIPRE Warning: Outbound Connection Alert

Your computer is trying to communicate with another computer in an untrusted zone.

Program:
c:\Users[redacted]\Downloads\AVC firewall tester\FirewallTester.exe

My Computer Address:
192.168.1.17:49166

Remote Computer Address:
[redacted]

Protocol:
TCP

Application rule name:
FirewallTester.exe

VIPRE has temporarily blocked this connection until you decide what action to take.

□ Take the action I choose in the future (create a rule)

What do you want to do?

Safe Mode

When we started our test PC in Safe Mode with Networking, we were able to open the VIPRE Internet Security window. Its status display indicated that real-time protection was disabled, but we were unable to reactivate it. The update function appeared to be working normally, however, which we find commendable. Custom and context-menu scans also functioned exactly as in standard mode, and removed all the items in our malware folder.

Help and documentation

Clicking the question-mark button in the top right-hand corner of VIPRE Internet Security's main window opens the local help service. This is a traditional Windows help file window with a list of topics in a pane on the left, and a larger right-hand pane to display the details of the topic selected.

There is a search function, with which we very quickly found clear and simple instructions for scheduling a scan. However, we were not able to find any details of how to set scan exceptions.

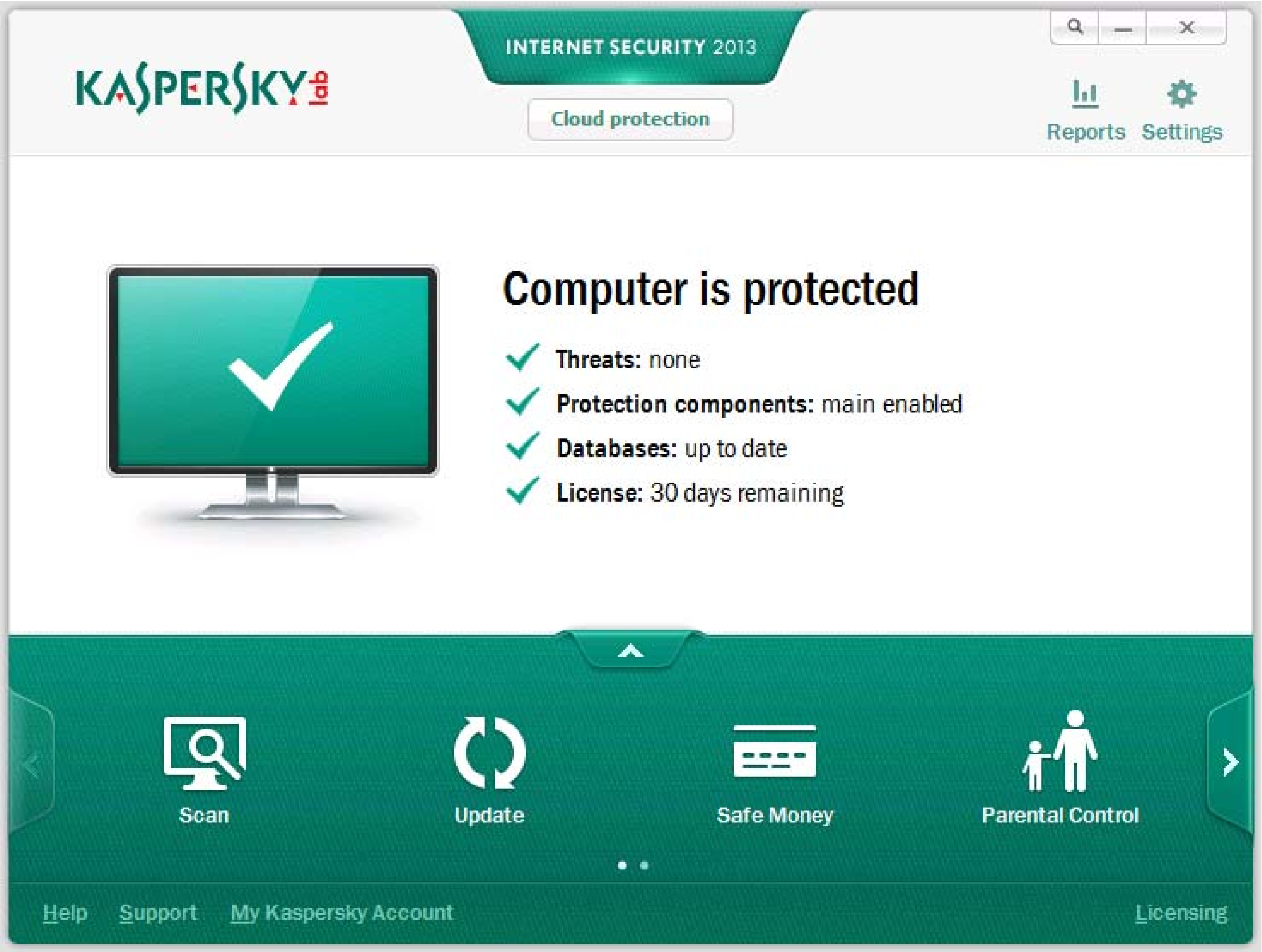
The VIPRE Product Support entry in the Help menu of VIPRE Internet Security opens the online knowledgebase of the VIPRE website. This also has a search function; again, this quickly provided an answer on how to schedule a scan, but drew a blank on scan exceptions/exclusions. Determined to find an answer to our second query, we resorted to doing a Google search; the first item on the results page was a link to VIPRE's FAQ page, which finally provided the answer we were looking for under the heading "Can I exclude a hard drive from VIPRE scans?". We searched both the local help and online knowledgebase again, this time using the word "exclude"; we were unsuccessful in both cases. To summarise, we suggest that VIPRE might be able to improve the search function in their help services.

We were unable to find a downloadable manual for the suite.

Verdict

VIPRE Internet Security 2013 is very easy to install. We found that the program window made all the important information and functions accessible, even if a little experimentation was required with some of the buttons and links in the component status sections. We were impressed with the vulnerability scan feature, although we feel its name ("Easy Update") is confusing. Default actions on malware discovery are good, and the fact that the program can update signatures in Safe Mode with Networking is a plus point. On the minus side, we were disappointed to see that real-time protection can be disabled easily using a non-administrator account. More worrying still is the fact that the firewall does not block incoming IPv6 traffic on untrusted (public) networks, meaning that there are no restrictions on pinging, file sharing and Remote Desktop access by an attacker who is using a default-configuration Windows Vista, 7 or 8 PC. We regard this as a serious flaw and urge the manufacturers to rectify it as soon as possible.

Kaspersky Internet Security 2013



Computer is protected

- ✓ **Threats:** none
- ✓ **Protection components:** main enabled
- ✓ **Databases:** up to date
- ✓ **License:** 30 days remaining

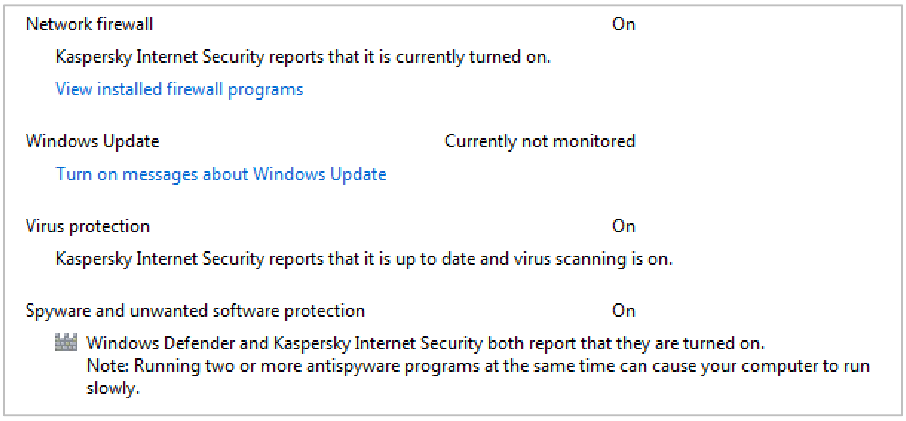
Components

Kaspersky Internet Security 2013 includes an antimalware component with email scanner, antispam, a firewall, and parental controls. Kaspersky tell us that the suite includes a feature called Automatic Exploit Prevention, which monitors the behaviour of applications with vulnerabilities, to prevent them causing any harm; and that another feature, Safe Money, can run websites in a protected mode to make online financial transactions more secure.

Installation

We installed Kaspersky Internet Security using the 168 MB full installer provided as a test version. We were pleased to see that this checks for a newer version before starting the installation process. The setup wizard's only option is whether to participate in Kaspersky's malware data sharing scheme. When the program first starts, the user is prompted to enter a licence key or opt for the trial version; we chose the latter. A reboot was not required.

Kaspersky Internet Security 2013 registers itself in Windows Action Center as an antivirus and antispyware program and firewall:



Network firewall On

Kaspersky Internet Security reports that it is currently turned on.

View installed firewall programs

Windows Update Currently not monitored

Turn on messages about Windows Update

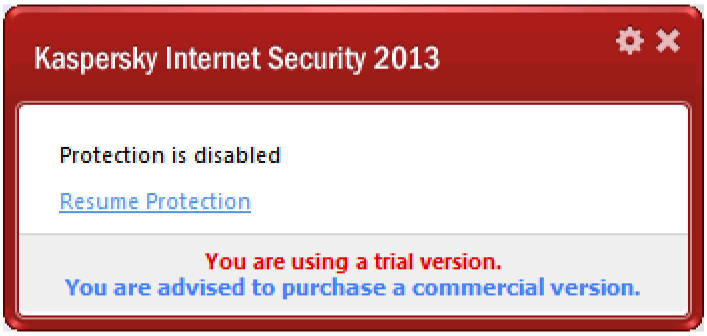
Virus protection On

Kaspersky Internet Security reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

Windows Defender and Kaspersky Internet Security both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

Windows Firewall is disabled, Windows Defender is not. If Kaspersky's real-time protection is disabled, Windows Action Center shows its normal alert, and Kaspersky additionally displays the following message, which we find commendable:



Kaspersky Internet Security 2013

Protection is disabled

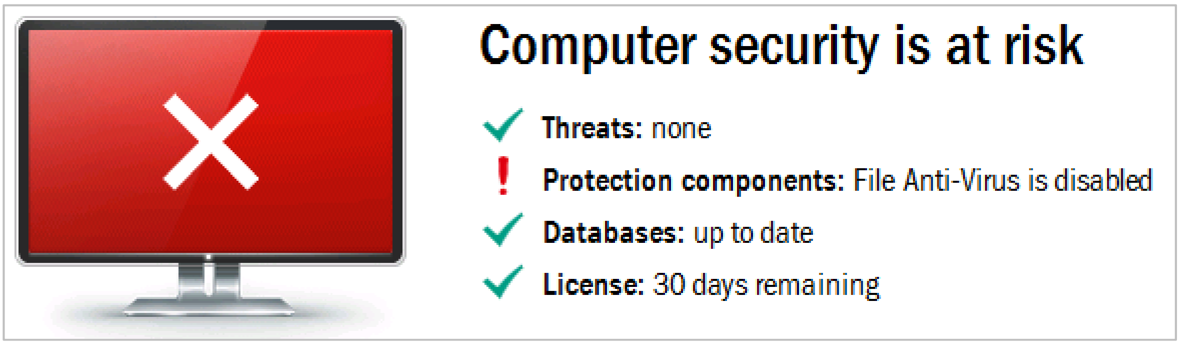
Resume Protection

You are using a trial version.
You are advised to purchase a commercial version.

Kaspersky's uninstaller program does not offer any options, only complete removal.

Program interface

The main program window of Kaspersky Internet Security 2013 is dominated by two horizontal stripes. The upper one is a status display, which shows whether important components are working properly and whether malware signatures are up to date. It also displays the number of days remaining for the current subscription. A big computer -screen icon also indicates the current protection status; if all is well, it displays a tick (checkmark) on a green background. Additionally, the bold status text at the top of the panel reads “Computer is protected”. If real-time protection is disabled, the text changes to “Computer security is at risk”, the icon shows a cross on red, and the Protection Components line indicates the nature of the problem (“File Anti-Virus is disabled”):



Computer security is at risk

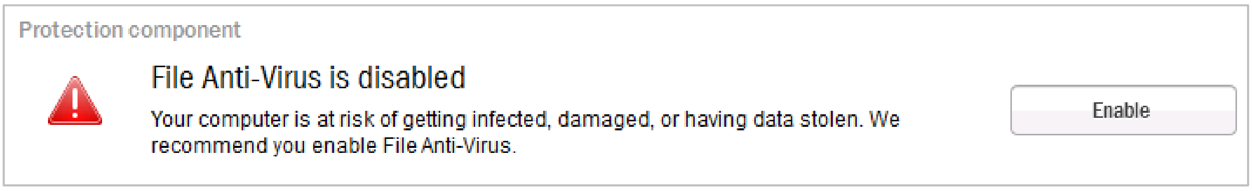
✓ **Threats:** none

! **Protection components:** File Anti-Virus is disabled

✓ **Databases:** up to date

✓ **License:** 30 days remaining

Although there is no Fix-All button as such, clicking anywhere in the upper panel displays a page with a detailed description of the problem, and a button to re-enable the protection:



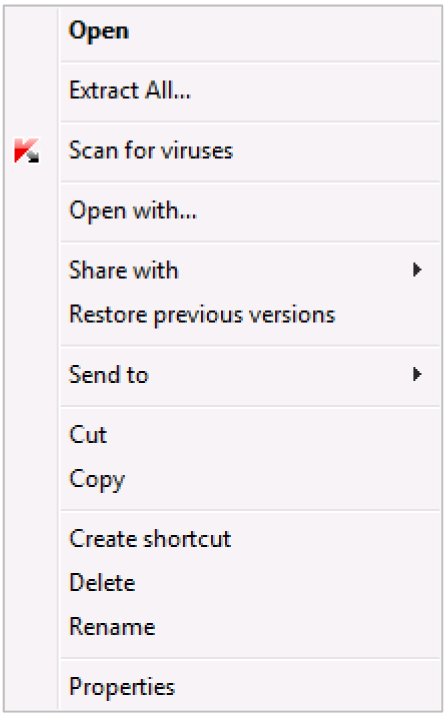
Protection component

File Anti-Virus is disabled

Your computer is at risk of getting infected, damaged, or having data stolen. We recommend you enable File Anti-Virus.

The lower panel of the main window displays large icons for important functions and features of the suite, including an Update Button and Scan button. The Scan button opens a page with four options: Full Scan, Critical Areas Scan (quick scan), Vulnerability Scan, and Custom Scan. We were pleased to note that a succinct description is provided for the first three of these, which we find very helpful.

Kaspersky adds a scan item to Windows Explorer's context menu:



The Help button in the bottom left-hand corner of the program's main window opens the local help feature. The Support button provides links to Kaspersky's online help services, local support tools and system information.

Default configuration

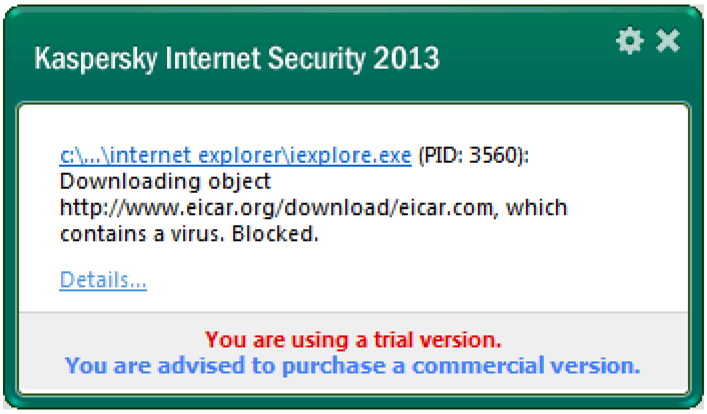
Non-administrator access

When we logged on to our test PC with a non-administrator account, we were able to deactivate real-time protection just as easily as when using an administrator account. We do not think this is ideal, especially in a suite designed for family use. It is possible to password-protect settings, but the setup wizard does not prompt the user to configure this.

Scanning and malware discovery

A scheduled scan is not set up by default in Kaspersky Internet Security 2013. It can be configured by going into Settings | Scan | Full Scan | Run Mode; we did not feel this was very easy to find, and suggest that a link on the Scan page of the program would be an improvement. We did not find a means of running a boot-time scan, although the Tools section allows a bootable rescue disk or drive to be created. A vulnerability scan is also available.

When we attempted to download the EICAR test file, Kaspersky blocked the web page and download, and displayed the following message:



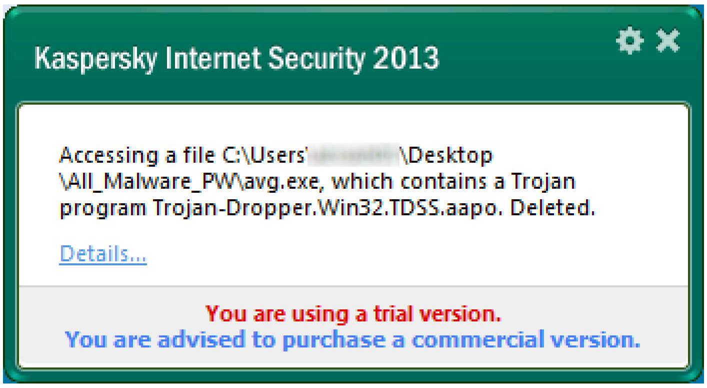
c:\...\internet explorer\iexplore.exe (PID: 3560):
Downloading object
http://www.eicar.org/download/eicar.com, which
contains a virus. Blocked.

Details...

You are using a trial version.
You are advised to purchase a commercial version.

Whilst this does state that the “virus” was blocked, and is quite appropriate for advanced users, we feel that a shorter, simpler message, stating clearly that no further action is required, would be better for non-experts.

When Kaspersky’ real-time protection discovered malware locally on our test PC, it quarantined it and showed this alert:



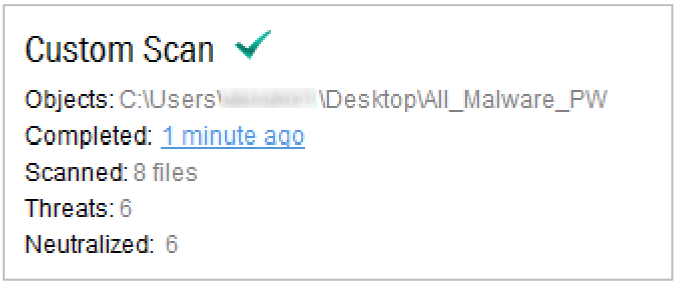
Accessing a file C:\Users\[redacted]\Desktop
\All_Malware_PW\avg.exe, which contains a Trojan
program Trojan-Dropper.Win32.TDSS.aapo. Deleted.

Details...

You are using a trial version.
You are advised to purchase a commercial version.

Again, we feel a shorter, simpler message would be better for non-expert users. However, we regard automatically quarantining the malware as an excellent default action.

When we ran a custom or context-menu scan on our folder of malware, Kaspersky summarised the results thus:


Custom Scan ✓

Objects: C:\Users\[redacted]\Desktop\All_Malware_PW
Completed: 1 minute ago
Scanned: 8 files
Threats: 6
Neutralized: 6

We would describe this as clear in one sense, namely that it shows all threats were neutralised. We found it a little unclear in another sense, namely that the light grey writing does not show up well on the white background. The malware is quarantined, meaning that expert users could recover an item if necessary.

Inbound firewall settings

After installing Kaspersky Internet Security 2013, we were able to access the test PC's file share, ping it, and log on using Remote Desktop, just as before. Changing the network type in Windows Network and Sharing Center from Work to Public had no effect, all three types of access remained open. However, when we connected to a new network and defined it as Public in the Windows new network prompt, we were not able to access the test PC over the network in any way.

Outbound firewall/application control

When we ran our firewall testing program, it completed its task without any warnings or hindrance. Kaspersky's application control is configured by assigning a program to a particular group; our firewall tester had automatically been put in the Low Restricted group, meaning not absolutely trusted, but allowed to run with limitations on data access and activities allowed. Manually assigning the program to the High Restricted group meant that it would open, but could not complete its download task; defining it as Untrusted prevented it from even opening.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were unable to open the Kaspersky Internet Security program window, meaning that we could not update signatures or run a custom scan. However, a context-menu scan ran exactly as it would in standard mode, removing all the malware and displaying the same results message box at the end.

Help and documentation

The local help feature uses a traditional Windows help file, with a list of topics in the left-hand pane, and a right-hand pane to display the details of the topic selected. There is a search function, which we used to look for answers to our two standard queries. Whilst we were able to find instructions for scheduling a scan fairly quickly, we feel that non-expert users might have some difficulty. The search turned up a number of topics, none of which actually included the word "schedule" in the title. We decided to investigate the "Full scan section" topic; the page displayed did not mention "schedule" either. However, clicking on "Run Mode" (an underlined subtitle in the text) opened up a panel with an explanation of the scheduling feature. We note, however, that the page does not include any instructions for finding the scan settings dialog, but assumes the user has already found it and wants to know what to do with it. We found articles relating to scan exclusions without much difficulty, but again these assumed the user had already found the dialog box concerned. In short, we feel the local help feature could be made more user-friendly for non-expert users.

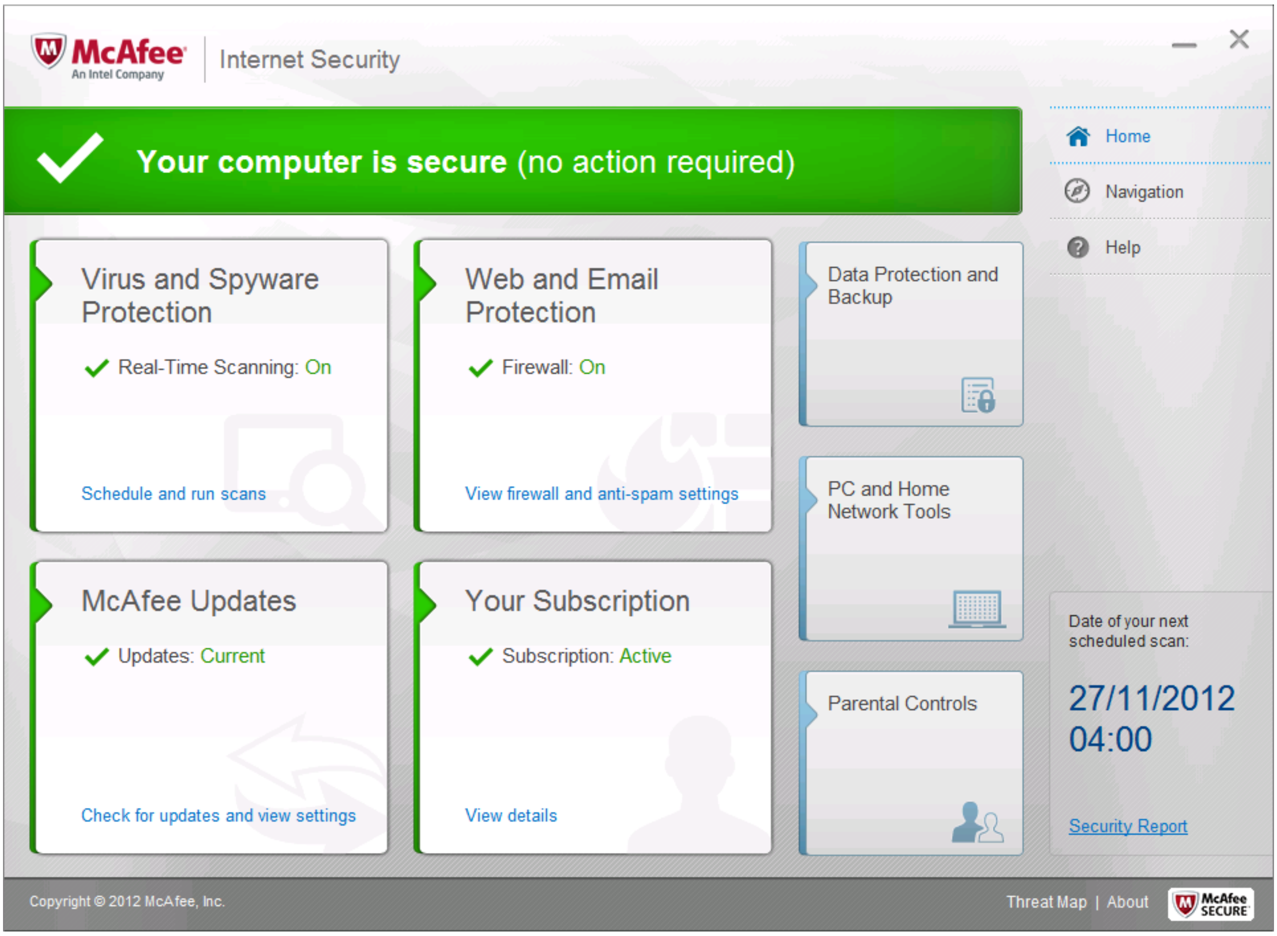
We found a knowledgebase for Internet Security 2013 on Kaspersky's international website, although it does not appear to have a search function. We would regard it as an FAQ page, with a somewhat limited range of common questions. One very useful feature of the knowledgebase is that there is a link to the English-language User-Guide, somewhat hidden in a screenshot of the program window; at the time of writing, (26th November 2012), we were unable to find the English version of the manual on the Home User Documentation page of Kaspersky's international or UK websites.

The User Guide is comprehensive, at 76 pages, and covers installation, configuration and use of the suite, along with details of the support options. There is an extensive table of contents with hyperlinks to the pages/sections concerned, and the document has been fully bookmarked, meaning any section can be easily found and opened using the Bookmarks Pane of Adobe Reader. The sections are laid out in a logical order, and we found the instructions/explanations to be clear and simple. There is only a modest number of screenshots, but these are clear and relevant.

Verdict

We found the main program window of Kaspersky Internet Security 2013 to be very well designed, making all important information and functions very easy to access. The program warns very effectively if real-time protection is switched off, and default actions on malware discovery are very good, even if we think some of the alert message-boxes could be a little simpler and clearer. A means of preventing non-administrator accounts from changing system settings would also be a welcome improvement. We feel the local help service could be improved somewhat, although the User Guide is excellent, if you are able to find it.

McAfee Internet Security 2013



McAfee An Intel Company | Internet Security

Your computer is secure (no action required)

Virus and Spyware Protection
✓ Real-Time Scanning: On
Schedule and run scans

Web and Email Protection
✓ Firewall: On
View firewall and anti-spam settings

Data Protection and Backup

PC and Home Network Tools

Parental Controls

McAfee Updates
✓ Updates: Current
Check for updates and view settings

Your Subscription
✓ Subscription: Active
View details

Date of your next scheduled scan:
27/11/2012 04:00
Security Report

Copyright © 2012 McAfee, Inc.

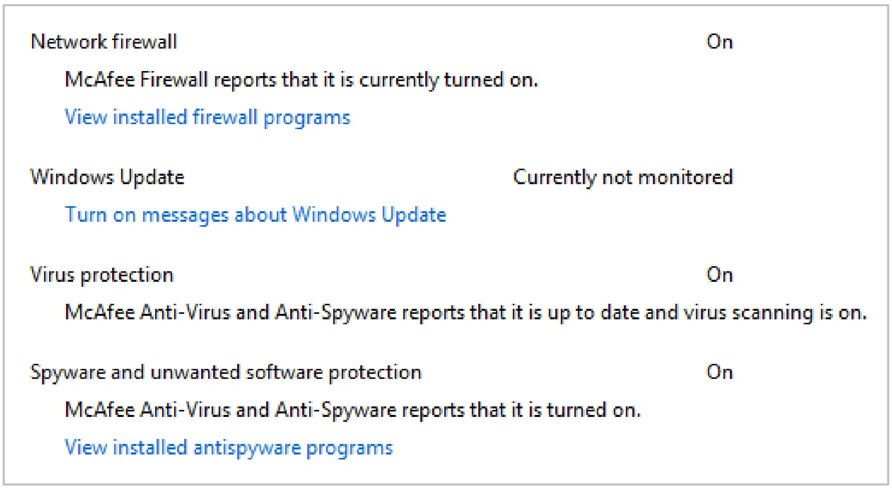
Components

McAfee Internet Security 2013 includes an antimalware component with email scanning, antispam, a firewall, plus parental controls, a shredder (secure data deletion) and a backup feature. There is also a “Home Network Manager” and “PC Tune Up” module.

Installation

We installed McAfee Internet Security 2013 from the 5 MB downloader file provided for the trial version. Setup involves entering the email address and password used to sign up for the trial, then deciding between Complete and Custom setup options. We chose the latter. This provides a full choice of the components to be installed. After downloading the complete software package to be installed, the wizard lets the user opt in or out of the malware data sharing program. A reboot is not required.

McAfee Internet Security 2013 registers itself in Windows Action Center as an antivirus and antispyware program and firewall. Windows Firewall and Windows Defender are disabled:



Network firewall On

McAfee Firewall reports that it is currently turned on.

View installed firewall programs

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

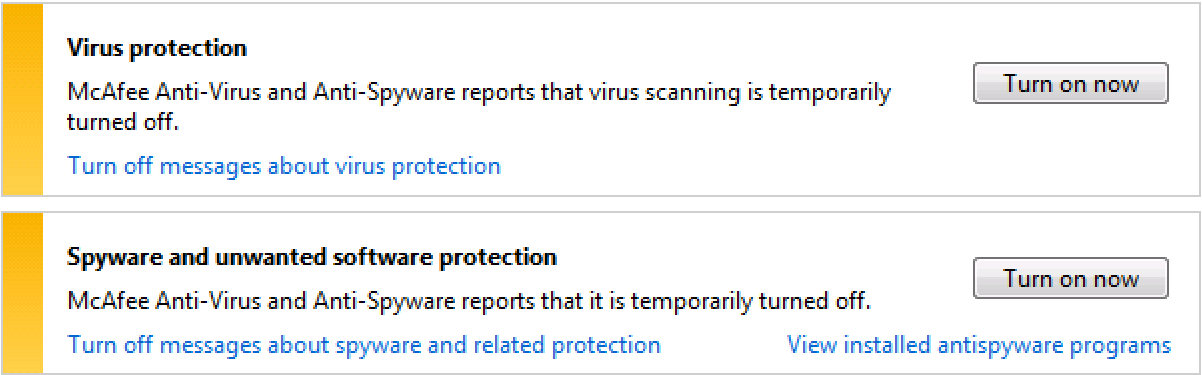
McAfee Anti-Virus and Anti-Spyware reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

McAfee Anti-Virus and Anti-Spyware reports that it is turned on.

View installed antispyware programs

When we disabled McAfee's real-time protection (choosing the option to permanently disable it), Windows Action Center produced only a muted warning as opposed to the full alert we would expect:



Virus protection

McAfee Anti-Virus and Anti-Spyware reports that virus scanning is temporarily turned off.

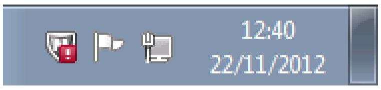
Turn off messages about virus protection

Spyware and unwanted software protection

McAfee Anti-Virus and Anti-Spyware reports that it is temporarily turned off.

Turn off messages about spyware and related protection View installed antispyware programs

The Windows Action Center icon did not change, or display the information bubble to warn that the antivirus was switched off. We note that McAfee's System Tray icon did change, however:



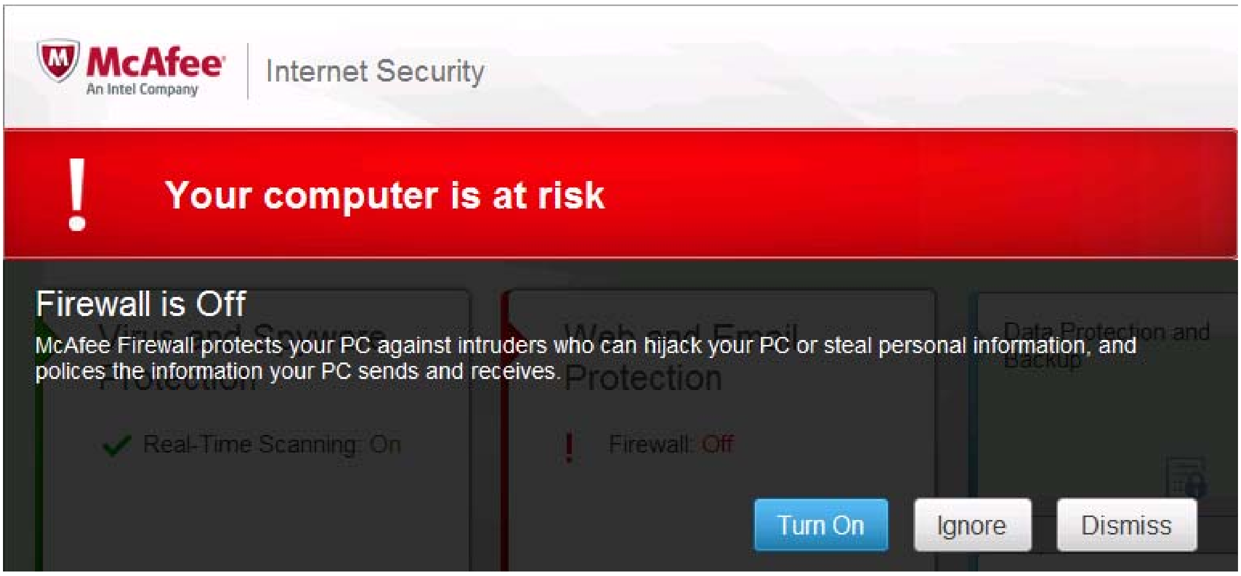
We feel that the muted warning from Windows Action Center is much less obvious than the standard warning message, and would not be apparent to users unless they deliberately checked the Action Center. We would urge McAfee to reconsider the suite's interaction with Action Center and implement the standard warning when important protection components are turned off.

McAfee's uninstaller program has very limited options. The only choice is to remove the SiteAdvisor (safe search) component separately from the rest of the suite, meaning users can uninstall SiteAdvisor and leave the rest of the suite, or vice versa. The only other possibility is complete removal. We could not find a repair feature.

Program interface

McAfee Internet Security 2013 has been completely redesigned, and its main program window is now dominated by tile-like buttons, reminiscent of Windows 8's Start Screen. There are four larger tiles, one each for the following features: Virus and Spyware Protection; Web and Email Protection; McAfee Updates; Your Subscription. Each of these has its own status line, the status text being shown in green if all is well. There are also 3 smaller tiles, entitled Data Protection and Backup; PC and Home Network Tools; Parental Controls.

Overall protection status is shown by means of a prominent horizontal strip at the top of the window. If all is well, this displays a tick (checkmark) and the text "Your computer is secure (no action required)" on green. When we switched off McAfee's real-time protection (specifying permanently), the status display text changed to an exclamation mark and the text "Your computer is at risk" on a red background. We were surprised to see that no Fix-All button, or any other obvious means of easily reactivating the protection, was displayed. However, when we switched the firewall off, a black panel appeared below the status display, displaying further information and providing a very obvious "Turn On" button:



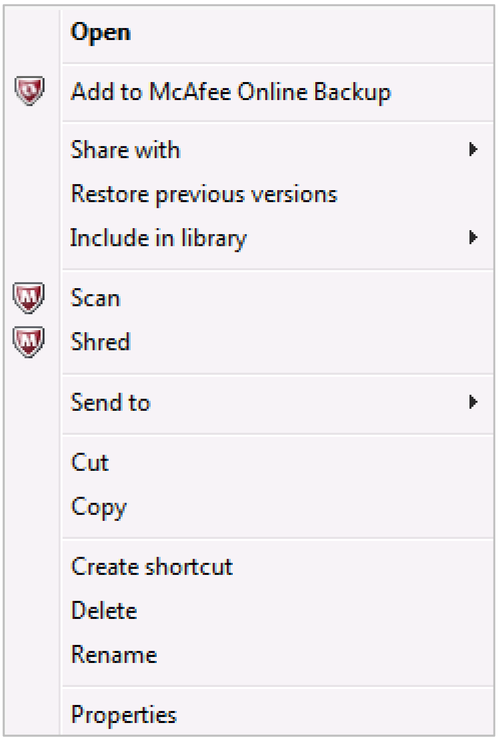
Firewall is Off

McAfee Firewall protects your PC against intruders who can hijack your PC or steal personal information, and polices the information your PC sends and receives.

We do not understand why McAfee have provided such a simple method for reactivating the firewall, but apparently not for real-time protection.

The suite's malware signatures can be easily updated by clicking the McAfee Updates tile on the home page. Scans can be run and scheduled by clicking the Virus and Spyware Protection tile.

McAfee Internet Security 2013 adds three entries to Windows Explorer's context menu, for backup, malware scanning and "shredding" (secure data deletion):



Subscription information can be found by clicking the Your Subscription tile on the home page, and the help functions are accessed by clicking the Help button in the top right-hand corner of the window.

Default configuration

Non-administrator access

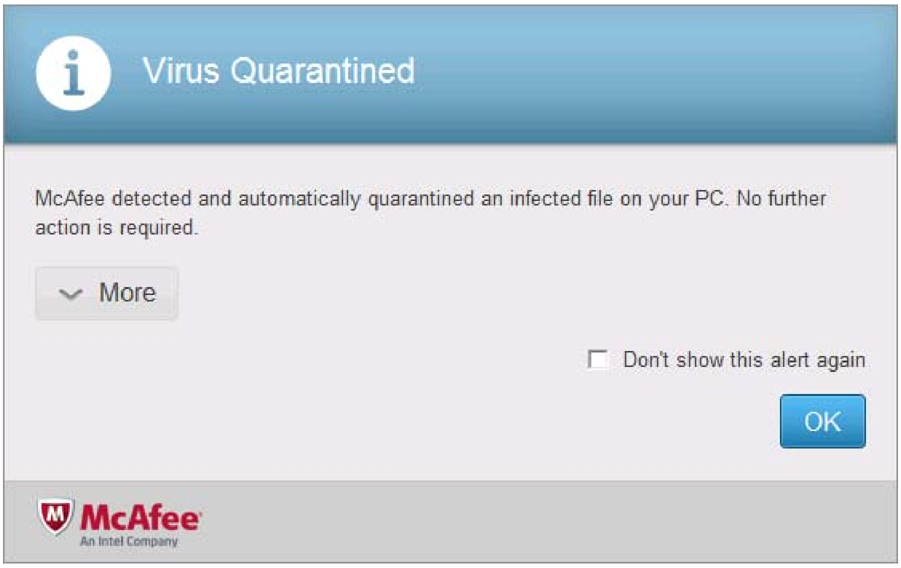
When we logged on to our test PC with a non-administrator account, we found the button for disabling real-time protection had been disabled, which we consider ideal.

Scanning and malware discovery

A scheduled scan is set by default, and McAfee is one of only a few programs to display the date and time of the next scheduled scan in the main program window. Whilst we find this commendable, we were a little disappointed to find that this area does not contain a link to the schedule settings, which would be very convenient. However, the Virus and Spyware Protection tile of the home page does include such a link, which makes it very easy to change the details of the scan.

It appears that the Custom Scan does not offer a means of selecting individual folders, other than standard system folders like Documents and Desktop. We could not find a means of running a boot-time scan.

When we attempted to download the EICAR test file, McAfee blocked the download and displayed the following message:



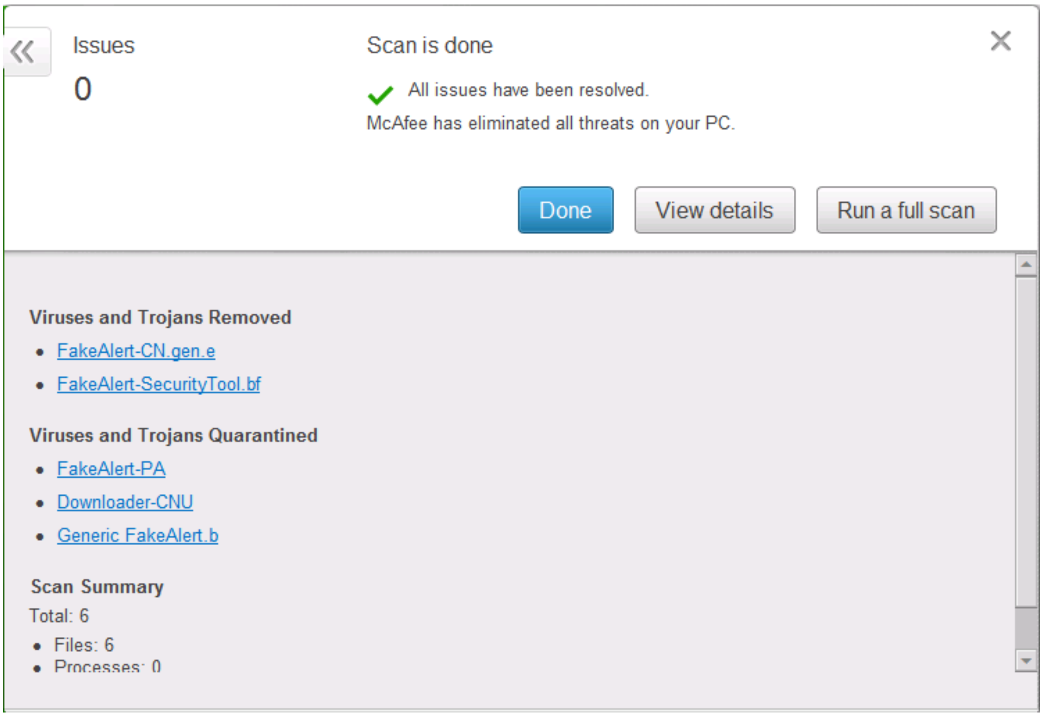
Virus Quarantined

McAfee detected and automatically quarantined an infected file on your PC. No further action is required.

This makes perfectly clear that the file has been quarantined, and the user does not need to take any further action. The More button allows users to see the name of the file and where it was discovered.

When malware was discovered locally by McAfee's real-time protection, it was quarantined automatically and a similar message to the one above was displayed; we note that McAfee's alerts use the correct terms for the malware discovered, so in the second case, the message read "Trojan Quarantined". We can only approve of this.

When we ran a context-menu scan or custom scan of the Desktop (where our malware folder was located), McAfee displayed the following results page:



Issues
0

Scan is done

✓ All issues have been resolved.

McAfee has eliminated all threats on your PC.

Viruses and Trojans Removed

- FakeAlert-CN.gen.e
- FakeAlert-SecurityTool.bf

Viruses and Trojans Quarantined

- FakeAlert-PA
- Downloader-CNU
- Generic FakeAlert.b

Scan Summary

Total: 6

- Files: 6
- Processes: 0

This makes clear that the malware has been made safe and that no further action is required, and provides details of the malware found and action taken.

Inbound firewall settings

When we installed McAfee Internet Security, we were not prompted to define the current network as public or private. We found that McAfee had evidently recognised the Work setting we were using for Windows Firewall, and translated this into the Work setting of its own firewall. After the installation, we were still able to access our test PC's file share, and log on using Remote Desktop. Rather surprisingly, we found that we could not ping it, with either IPv4 or IPv6 (though we later found that responding to pings can be enabled or disabled in the firewall settings). When we changed the network type to Public in Windows Network and Sharing Center, we found that this automatically changed the setting in McAfee's firewall to Public as well. We were then unable to access the file share from another PC on the network. When we tried to log on to the test PC using Remote Desktop, we found that using the computer's hostname failed, but using its IP address allowed access. We would suggest that the latter is a flaw in the firewall, and should be rectified.

Changing the network type back to Work in Windows also changed it to Work in McAfee's firewall, enabling full access once again. We find this ideal.

Outbound firewall/application control

When we ran our firewall testing program, McAfee's firewall allowed it to complete its task without any sort of query. We were unable to find a mode which would ask the user before allowing the program to connect to the Internet; both Monitored Access and Stealth modes state that the user will be asked when *unknown* programs try to connect, so we assume that McAfee correctly recognised that the program is harmless.

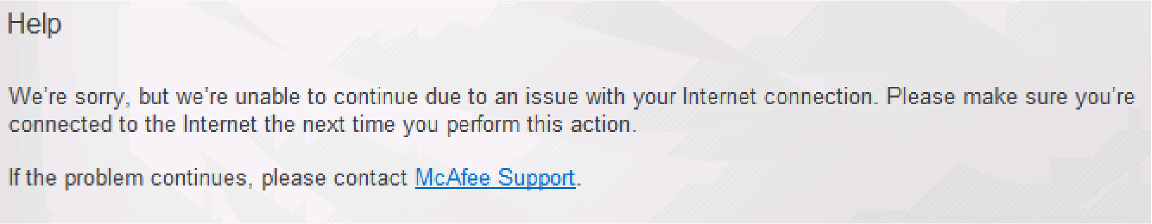
Safe Mode

When we started our test PC in Safe Mode with Networking, we were able to open the McAfee Internet Security program window. Although this advised us that real-time protection was disabled, we were able to use the update function to update the signatures; the program confirmed that this had worked by displaying the correct day and time for the last successful update. We regard McAfee's ability to update signatures in Safe Mode with Networking as excellent.

Having updated the definitions, we found we were able to run custom or context-menu scans and remove the malware samples in exactly the same way as in standard mode.

Help and documentation

When we clicked on the Help link on the Help page of McAfee Internet Security, we were confronted with the following message:



Help

We're sorry, but we're unable to continue due to an issue with your Internet connection. Please make sure you're connected to the Internet the next time you perform this action.

If the problem continues, please contact McAfee Support.

We confirmed that an Internet connection was available by successfully opening the McAfee website and pinging www.mcafeee.com.

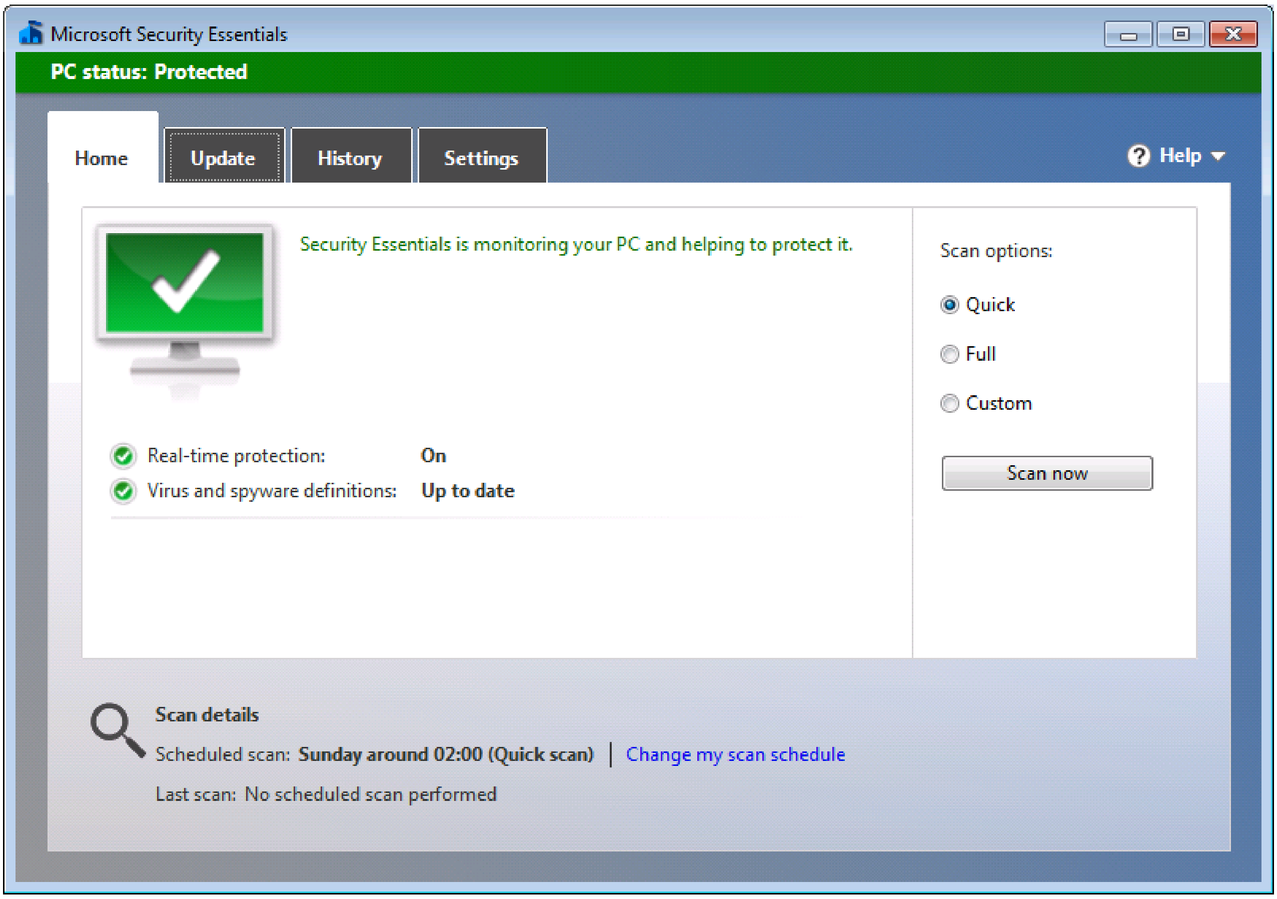
We used the search function in the FAQ section of McAfee's support website to attempt to find answers to our two standard queries. At the time of writing, late November 2012, we were unable to find answers relating to the 2013 version of McAfee Internet Security. Although there were suitable answers for earlier versions of the product, these do not apply to the redesigned interface in the current version.

We were unable to find a manual for McAfee Internet Security 2013. We assume that McAfee has not yet updated its help services to cover the new release of Internet Security.

Verdict

We found the new interface of McAfee Internet Security 2013 to be very well designed, making all important features and information easily accessible. Alerts and default actions on malware discovery also impressed us, as did the ability to update malware signatures in Safe Mode. However, we also found some aspects which we feel could be improved, such as the muted Action Center warning and the ability to log on to the PC with Remote Desktop in Public mode if the IP address is used. At the time of writing, it appeared that the (online) help features had not yet been made available.

Microsoft Security Essentials 4.1



PC status: Protected

Security Essentials is monitoring your PC and helping to protect it.

Real-time protection: On
Virus and spyware definitions: Up to date

Scan options:
● Quick
○ Full
○ Custom

Scan details
Scheduled scan: **Sunday around 02:00 (Quick scan)** | Change my scan schedule
Last scan: No scheduled scan performed

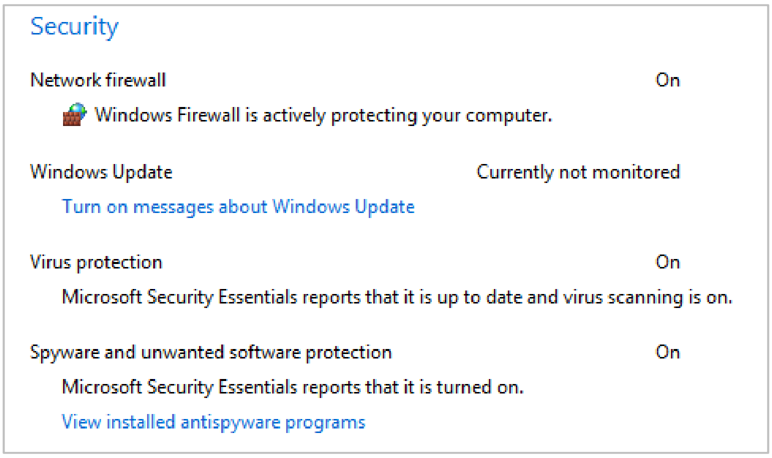
Components

Microsoft Security Essentials is a simple antimalware program without any additional components.

Installation

To install Microsoft Security Essentials, we downloaded a 13 MB installer file. The installation process is very simple, with few options. There is the usual licence agreement to accept, the opportunity to opt in to Microsoft's Customer Experience Improvement Program, and the chance to accept Microsoft's recommendation to turn on Windows Firewall if no other firewall is used. There is a warning to uninstall any other antivirus software, and the chance to run a scan when the program has installed and updated. We estimate that the installation was completed in about a minute. A reboot was not required.

Microsoft Security Essentials registers itself in Windows 7's Action Center as an antivirus and antispyware program. Windows Defender is disabled, Windows Firewall is not.



Security

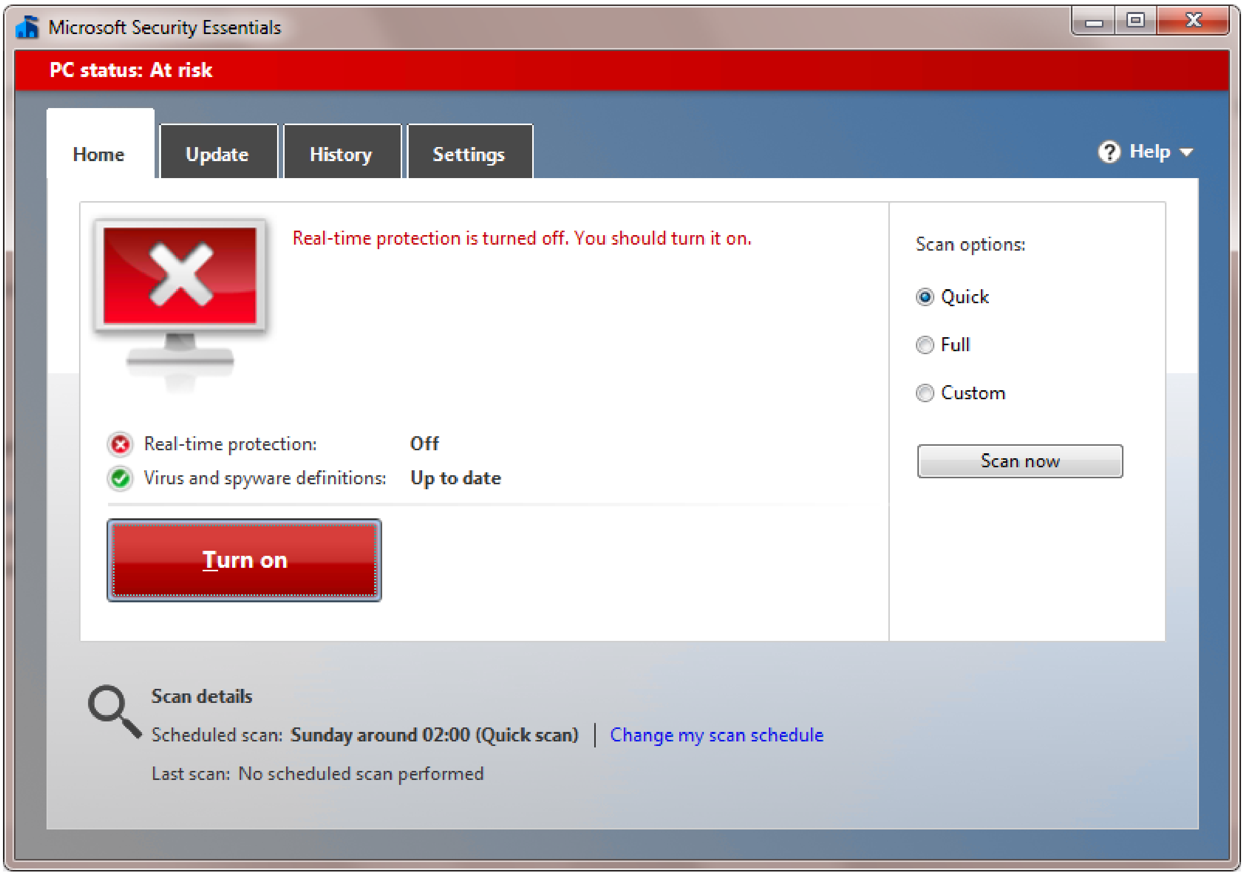
Network firewall	On
Windows Firewall is actively protecting your computer.	
Windows Update	Currently not monitored
Turn on messages about Windows Update	
Virus protection	On
Microsoft Security Essentials reports that it is up to date and virus scanning is on.	
Spyware and unwanted software protection	On
Microsoft Security Essentials reports that it is turned on.	
View installed antispyware programs	

If the real-time protection of Microsoft Security Essentials is turned off, Action Center immediately shows an alert.

The program's uninstaller has no options; only a complete removal is possible.

Program interface

The Home page of Microsoft Security Essentials shows the current protection status, in the form of a computer-screen icon with a tick (checkmark) on green, and the word "Protected" above, if all is well. If real-time protection is disabled, the icon shows a cross on red, the text changes to "At risk", and a big red button marked "Turn on" appears below:



PC status: At risk

Real-time protection is turned off. You should turn it on.

Real-time protection:	Off
Virus and spyware definitions:	Up to date

Scan options:

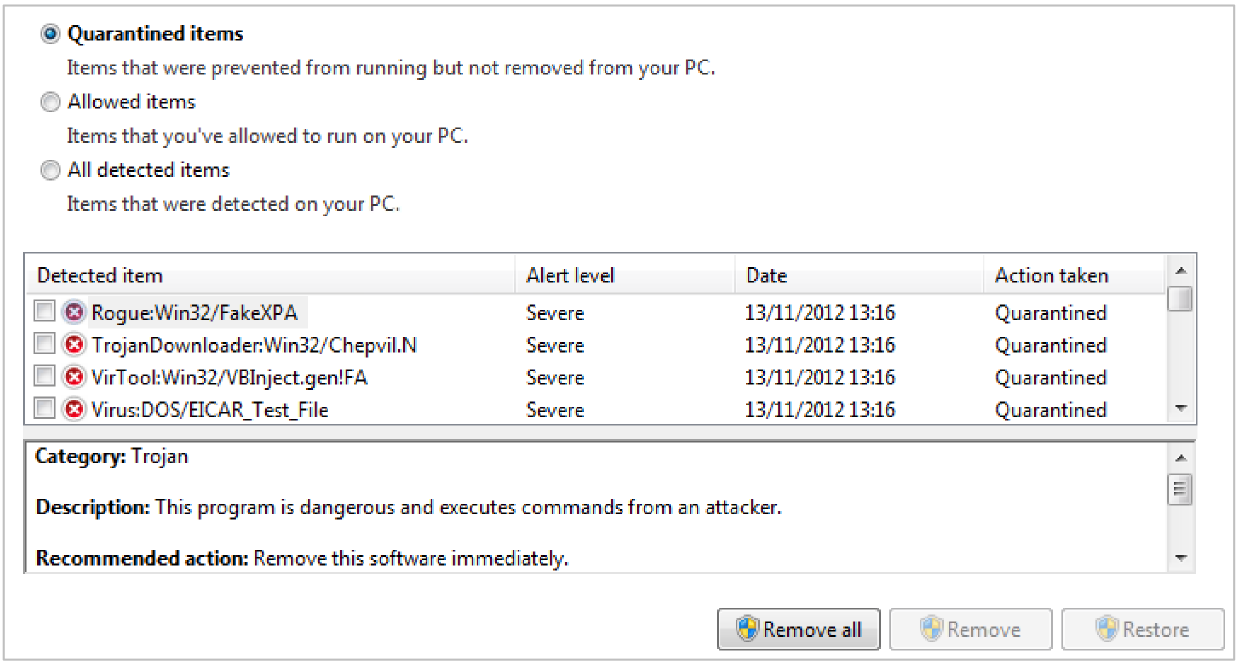
● Quick
○ Full
○ Custom

Scan details

Scheduled scan: Sunday around 02:00 (Quick scan) | Change my scan schedule

Last scan: No scheduled scan performed

The scan options, namely Quick, Full and Custom, are available in a separate panel on the right-hand side of the Home page. Details of the next scheduled scan, and a link to the scheduler, are displayed at the bottom of the window. Three other pages are available, namely Update, History, and Settings, and these are accessed via tabs at the top of the window. The Update page only has one functional control, a big button marked Update, but also displays information about virus and spyware definition versions and dates. History shows a list of all malware items found, with a filter that allows quarantined items to be displayed and deleted:



● **Quarantined items**
Items that were prevented from running but not removed from your PC.
○ Allowed items
Items that you've allowed to run on your PC.
○ All detected items
Items that were detected on your PC.

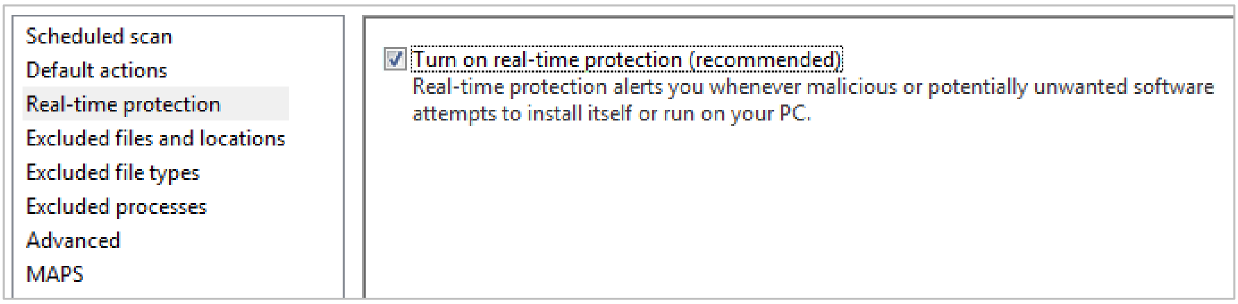
Detected item	Alert level	Date	Action taken
□ Rogue:Win32/FakeXPA	Severe	13/11/2012 13:16	Quarantined
□ TrojanDownloader:Win32/Chepvil.N	Severe	13/11/2012 13:16	Quarantined
□ VirTool:Win32/VBInject.gen!FA	Severe	13/11/2012 13:16	Quarantined
□ Virus:DOS/EICAR_Test_File	Severe	13/11/2012 13:16	Quarantined

Category: Trojan

Description: This program is dangerous and executes commands from an attacker.

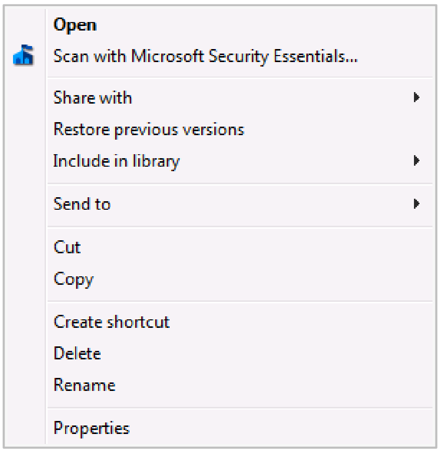
Recommended action: Remove this software immediately.

Settings displays a clear and simple list of configurable items and their options:



☑ Turn on real-time protection (recommended)
Real-time protection alerts you whenever malicious or potentially unwanted software attempts to install itself or run on your PC.

Microsoft Security Essentials is integrated into Windows Explorer by means of a Scan entry in the context menu:



As Microsoft Security Essentials is a free program, there is no subscription and thus no subscription information.

Help is accessible from a button of the same name in the top right-hand corner of the window.

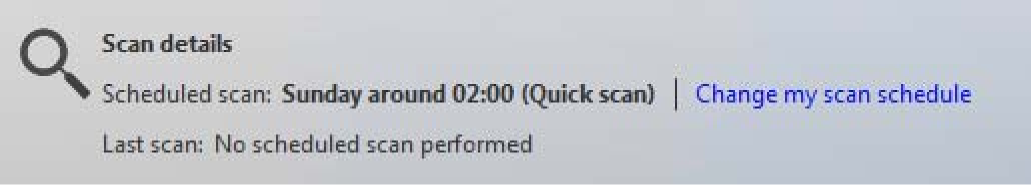
Default configuration

Non-administrator access

When we logged on to our test PC with a non-administrator account, we were unable to disable the real-time protection, as a Windows User Account Control dialog box demand administrator credentials. We regard this as ideal.

Scanning and malware discovery

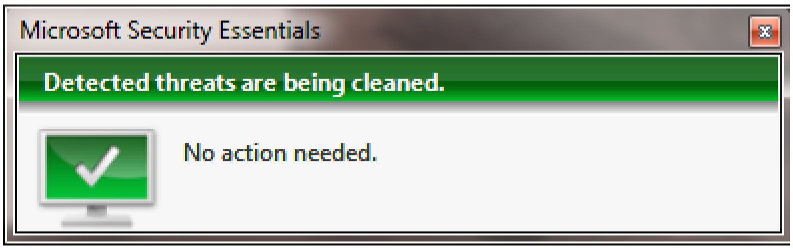
Microsoft Security Essentials sets a scheduled scan by default, and takes the innovative step of displaying the day, time and type of the next scheduled scan on the home page of the program window, which we found commendable. There is also a link to the schedule settings page:


Scan details

Scheduled scan: **Sunday around 02:00 (Quick scan)** | Change my scan schedule

Last scan: No scheduled scan performed

When we attempted to download the EICAR test file, this was blocked, and the following message displayed:



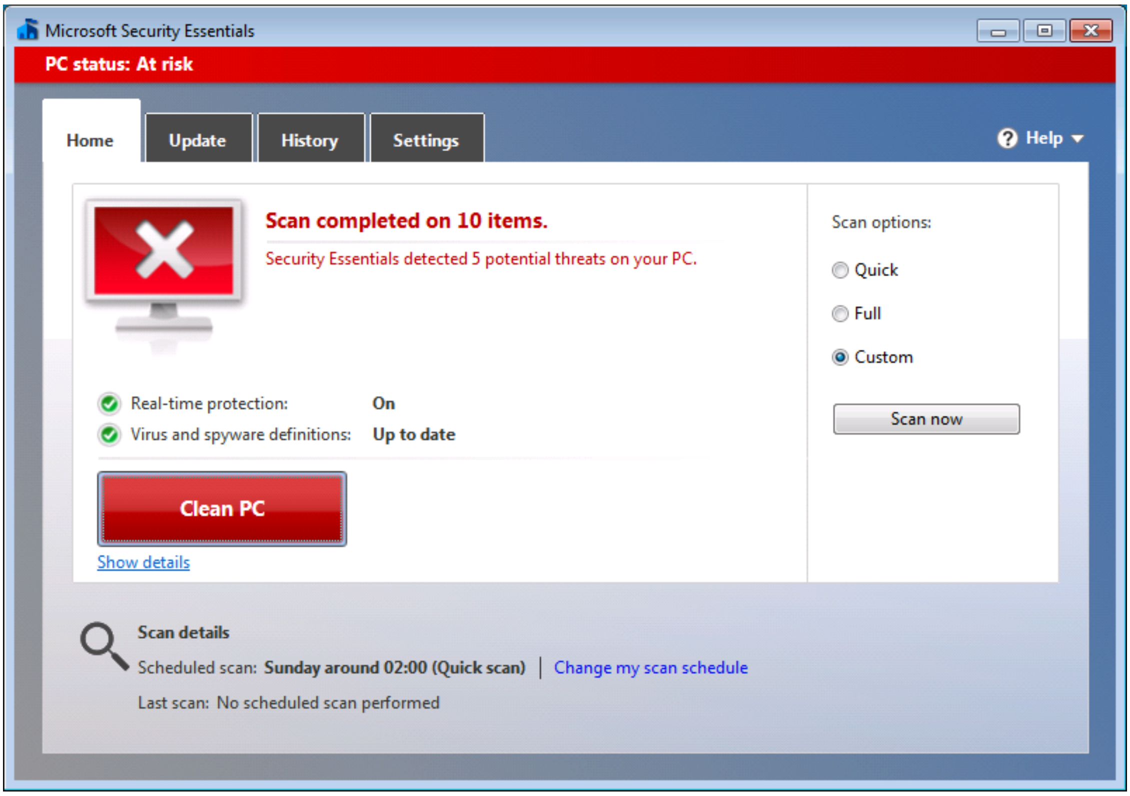
Microsoft Security Essentials

Detected threats are being cleaned.

No action needed.

The same message was shown when malware was discovered locally on our test PC by the real-time protection. We note that although Microsoft Security Essentials completely prevented any malware items from executing, and quarantined the threats successfully, it appeared to be very slow in deleting the malware; it took over a minute for a single item to be deleted, compared to a few seconds at most for the majority of programs in the review.

When we ran a custom or context-menu scan on our malware folder, Microsoft Security Essentials indicated that it had found malware, and presented a very obvious red button marked “Clean PC” to remove it, along with a more subtle link marked “Show details”:



Microsoft Security Essentials

PC status: At risk

Scan completed on 10 items.

Security Essentials detected 5 potential threats on your PC.

Real-time protection: On

Virus and spyware definitions: Up to date

Scan options:

○ Quick

○ Full

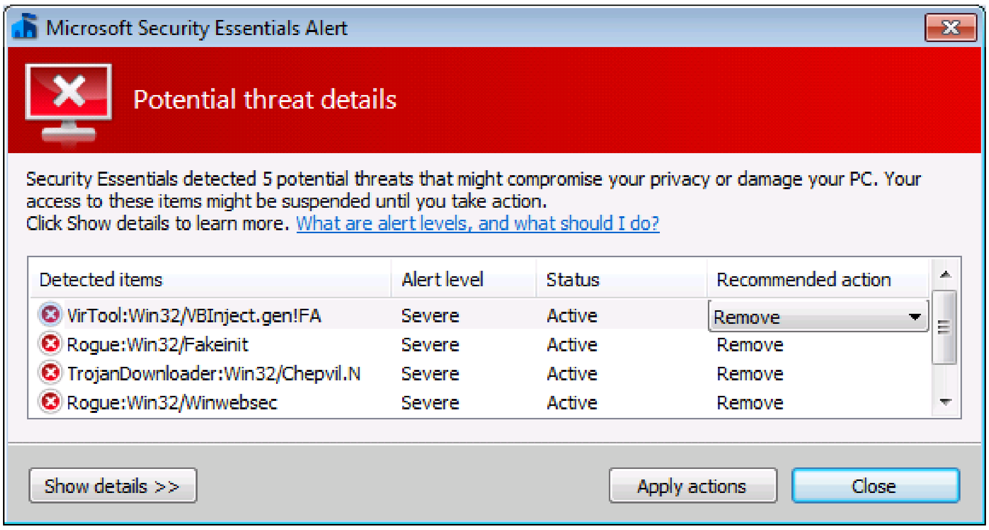
● Custom

Scan details

Scheduled scan: Sunday around 02:00 (Quick scan) | Change my scan schedule

Last scan: No scheduled scan performed

Clicking on Show Details displayed a list of the malware items found, along with the opportunity to change the default action (Remove):



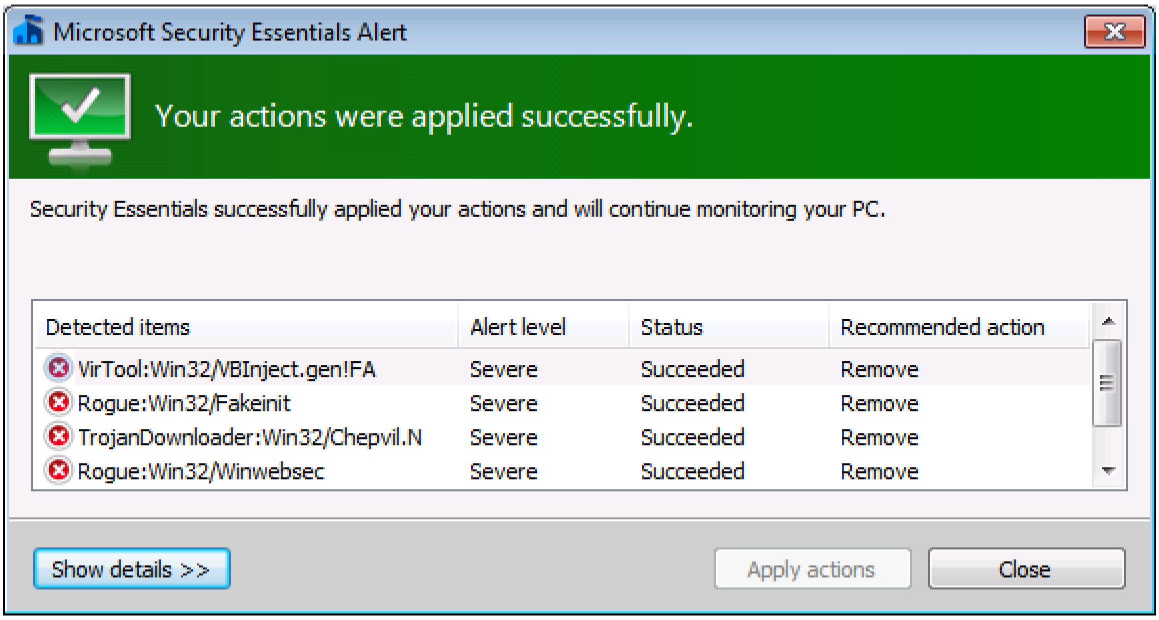
Microsoft Security Essentials Alert

Potential threat details

Security Essentials detected 5 potential threats that might compromise your privacy or damage your PC. Your access to these items might be suspended until you take action.
Click Show details to learn more. What are alert levels, and what should I do?

Detected items	Alert level	Status	Recommended action
VirTool:Win32/VBInject.gen!FA	Severe	Active	Remove
Rogue:Win32/Fakeinit	Severe	Active	Remove
TrojanDownloader:Win32/Chepvil.N	Severe	Active	Remove
Rogue:Win32/Winwebsec	Severe	Active	Remove

Clicking on Clean PC in the main program window removed all the malware items and displayed the results:



Microsoft Security Essentials Alert

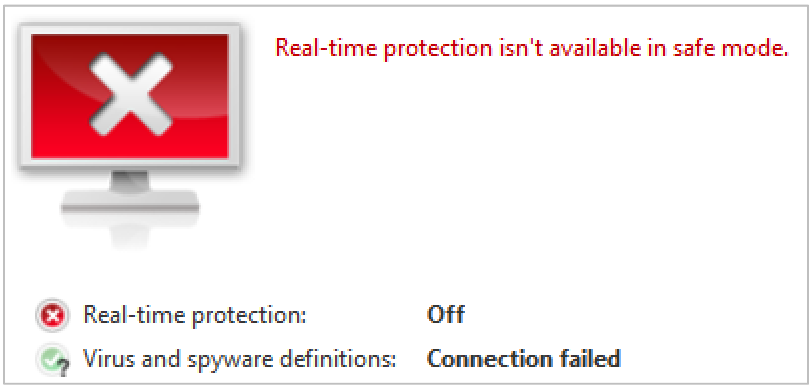
Your actions were applied successfully.

Security Essentials successfully applied your actions and will continue monitoring your PC.

Detected items	Alert level	Status	Recommended action
VirTool:Win32/VBInject.gen!FA	Severe	Succeeded	Remove
Rogue:Win32/Fakeinit	Severe	Succeeded	Remove
TrojanDownloader:Win32/Chepvil.N	Severe	Succeeded	Remove
Rogue:Win32/Winwebsec	Severe	Succeeded	Remove

Safe Mode

When we started our test PC in Safe Mode with Networking and opened Microsoft Security Essentials, we found that its home page helpfully informed us of the features that were not available, namely updating and real-time protection:



Real-time protection isn't available in safe mode.

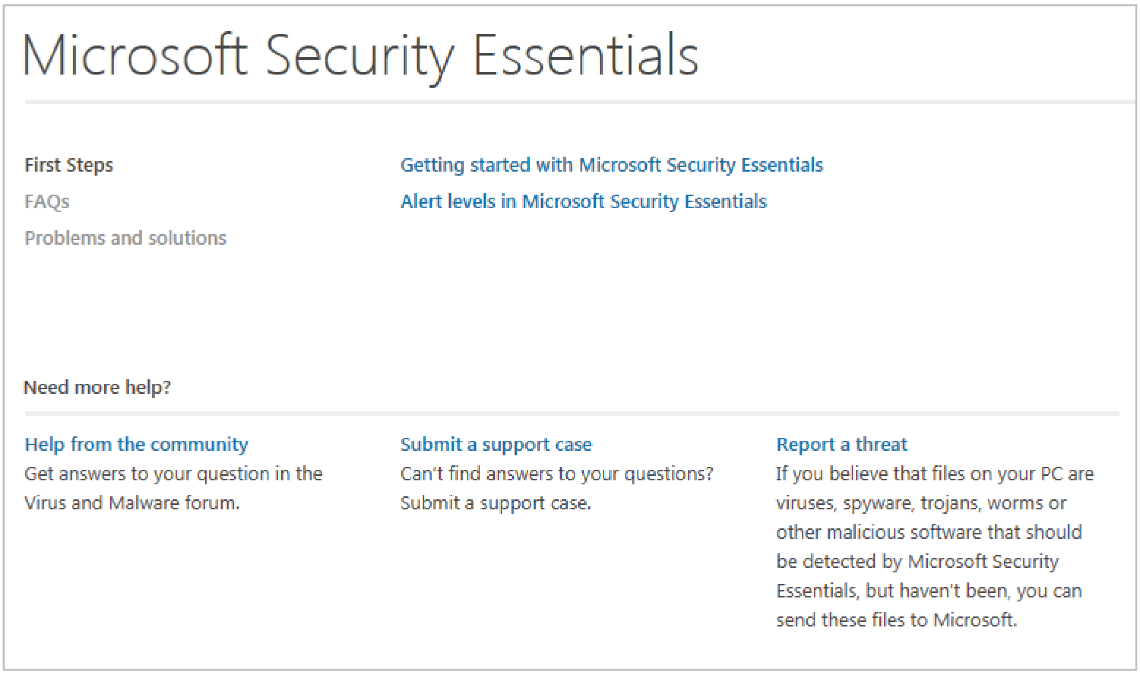
Real-time protection: Off

Virus and spyware definitions: Connection failed

We were able to run custom and context-menu scans on our malware folder, and remove the items found, just the same as in standard mode.

Help and documentation

We were able to run custom and context-menu scans on our malware folder, and remove the items found, just the same as in standard mode. Microsoft informed us that Windows Defender Offline, which can be downloaded and made into a bootable CD/DVD/flash drive, is their recommended tool for removing malware that cannot be deleted in standard mode.



Microsoft Security Essentials

First Steps

FAQs

Problems and solutions

Getting started with Microsoft Security Essentials

Alert levels in Microsoft Security Essentials

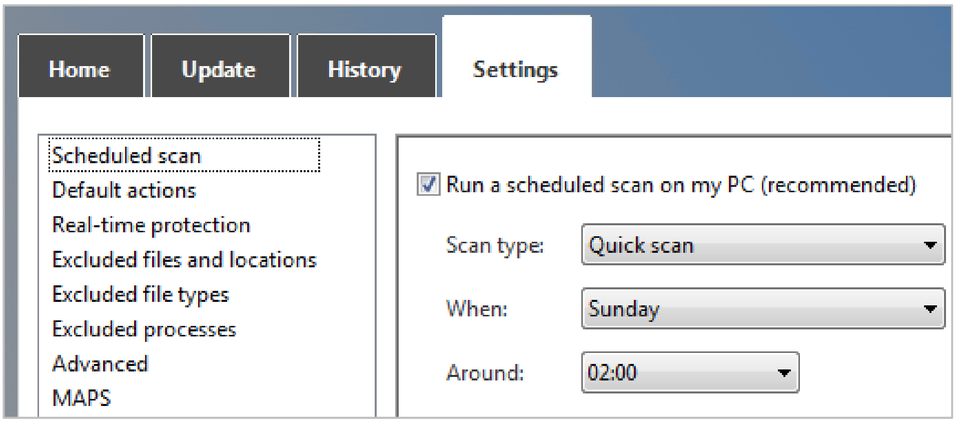
Need more help?

Help from the community
Get answers to your question in the Virus and Malware forum.

Submit a support case
Can't find answers to your questions? Submit a support case.

Report a threat
If you believe that files on your PC are viruses, spyware, trojans, worms or other malicious software that should be detected by Microsoft Security Essentials, but haven't been, you can send these files to Microsoft.

The FAQs and “Problems and solutions” pages only display about half a dozen items each, not including our queries on scheduling a scan or settings can exclusions. However, the “Help from the community" section has a search function which allows specific questions to be asked. This quickly led us to instructions on how to schedule a scan. Whilst we did not find an ideal answer to the query on setting scan exclusions, we feel that the relevant menu item (Excluded Files and Locations) is so easy to find on the Settings page that no instructions are really necessary:



☑ Run a scheduled scan on my PC (recommended)

Scan type: Quick scan

When: Sunday

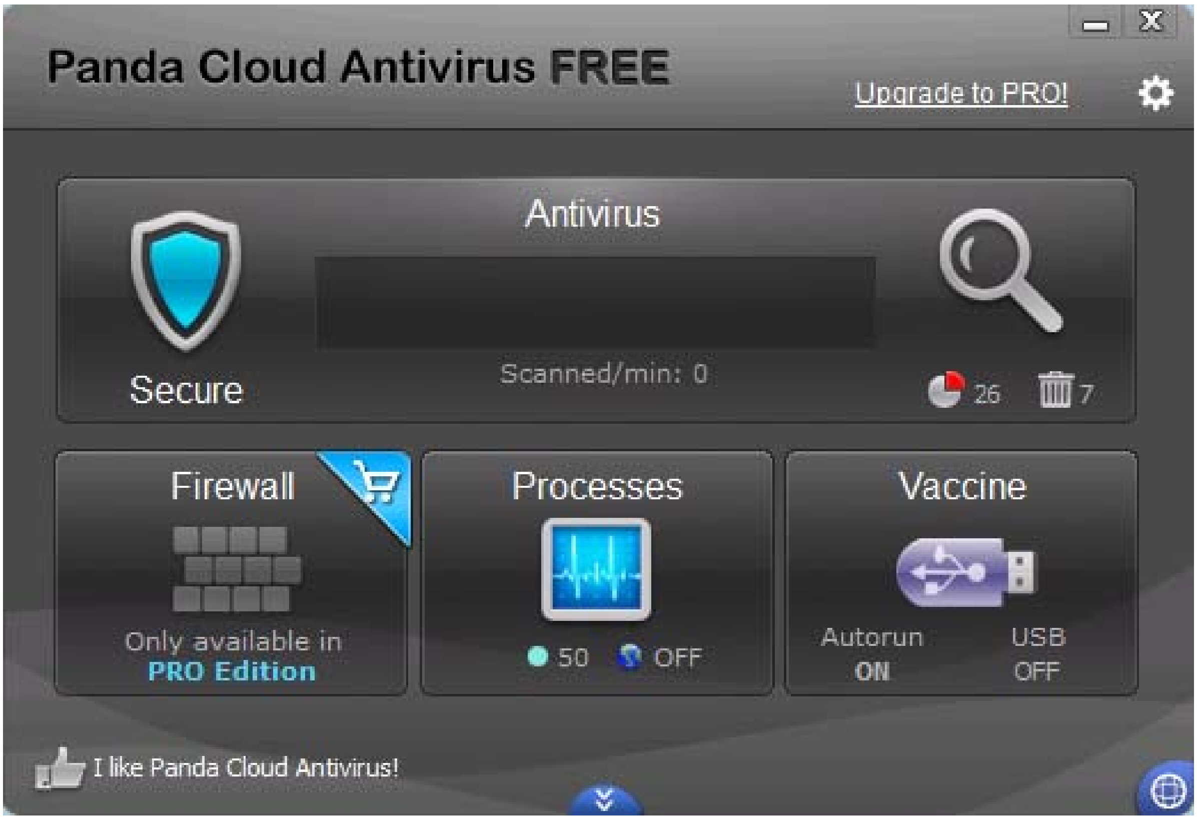
Around: 02:00

We were unable to find a separate manual for the program.

Verdict

Microsoft Security Essentials is a basic antimalware program with essential functionality. Within the limits of its scope, we found it to be very well designed, making essential information and tasks easily available to the user in a clear and simple interface. We particularly liked the fact that information on the next scheduled scan, along with a link to the scheduler, is displayed on the program's home page.

Panda Cloud Antivirus Free 2.0.1



Panda Cloud Antivirus FREE

Upgrade to PRO!

Antivirus

Secure

Scanned/min: 0

26 7

Firewall

Only available in PRO Edition

Processes

50 OFF

Vaccine

Autorun ON

USB OFF

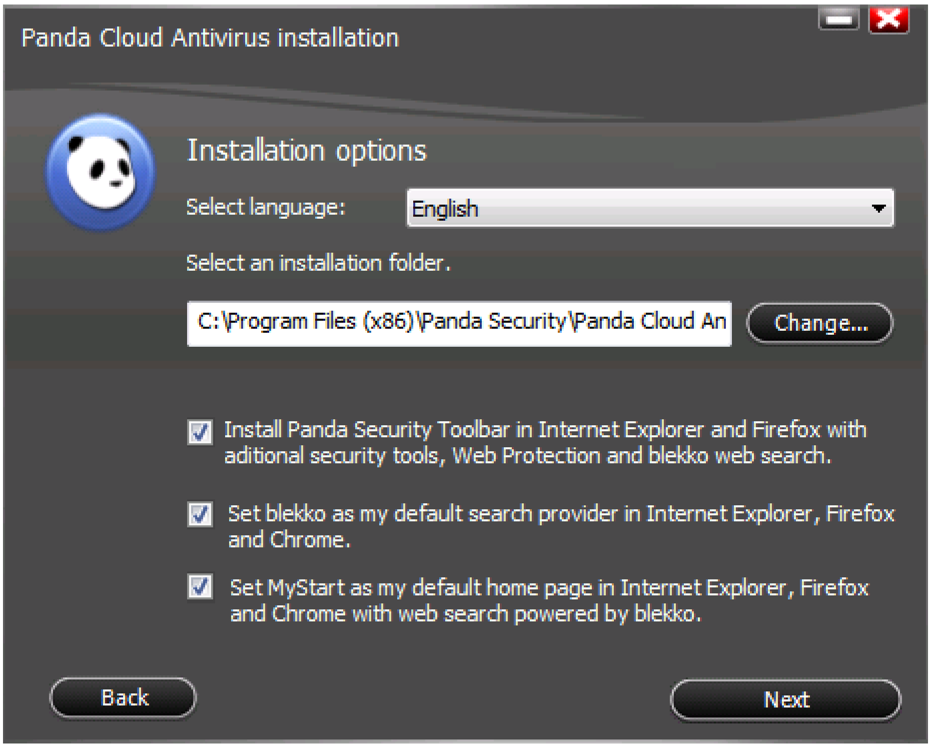
I like Panda Cloud Antivirus!

Components

Panda Cloud Antivirus Free is an antimalware program without an email scanner.

Installation

We installed Panda Cloud Antivirus Free using a 790 KB downloader file, which we downloaded from www.cloudantivirus.com (rather than Panda's main website, www.pandasecurity.com). The installation wizard requires the acceptance of a licence agreement, then provides a number of options on a single page. These are language (there is a choice of major European and Asian languages); the installation folder location; the installation of the Panda Security Toolbar; using Blekko as the default search provider; and using a home page called MyStart.



Panda Cloud Antivirus installation

Installation options

Select language: English

Select an installation folder.

C:\Program Files (x86)\Panda Security\Panda Cloud An

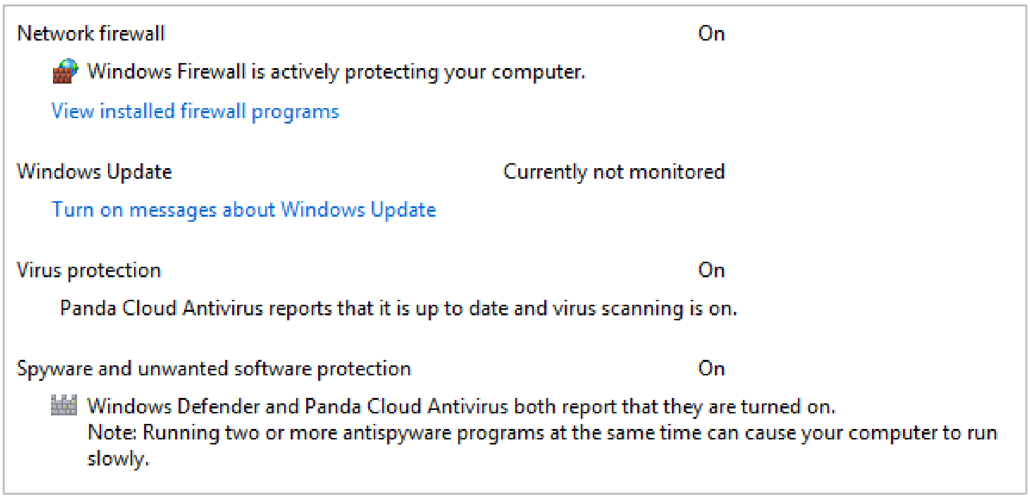
☑ Install Panda Security Toolbar in Internet Explorer and Firefox with aditional security tools, Web Protection and blekko web search.

☑ Set blekko as my default search provider in Internet Explorer, Firefox and Chrome.

☑ Set MyStart as my default home page in Internet Explorer, Firefox and Chrome with web search powered by blekko.

In line with our standard installation policy, we declined to use Blekko as the search provider, and MyStart as the home page, as these appeared to be third-party offerings; however, Panda have since informed us that they were joint developers of the URL filter. No other options were offered. At the end of the installation wizard, the user is offered the choice of using the Free or Pro editions of Panda Cloud Antivirus, naturally we chose Free. A reboot was not required.

Panda Cloud Antivirus Free registers itself in Windows Action Center as an antivirus and antispyware program. Neither Windows Firewall nor Windows Defender is disabled:



Network firewall On

Windows Firewall is actively protecting your computer.

View installed firewall programs

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

Panda Cloud Antivirus reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

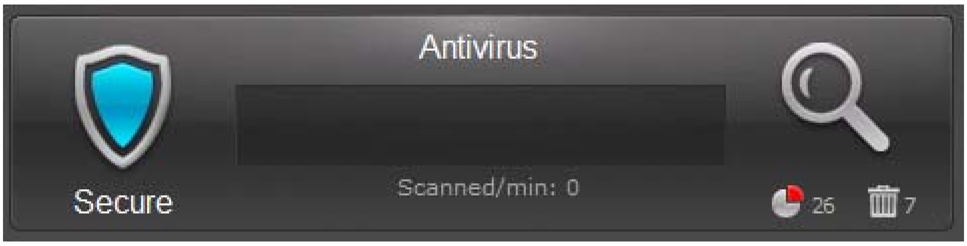
Windows Defender and Panda Cloud Antivirus both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

Disabling the real-time protection in Cloud Antivirus Free causes Windows Action Center to show its normal alert.

The uninstaller program has no options other than complete removal.

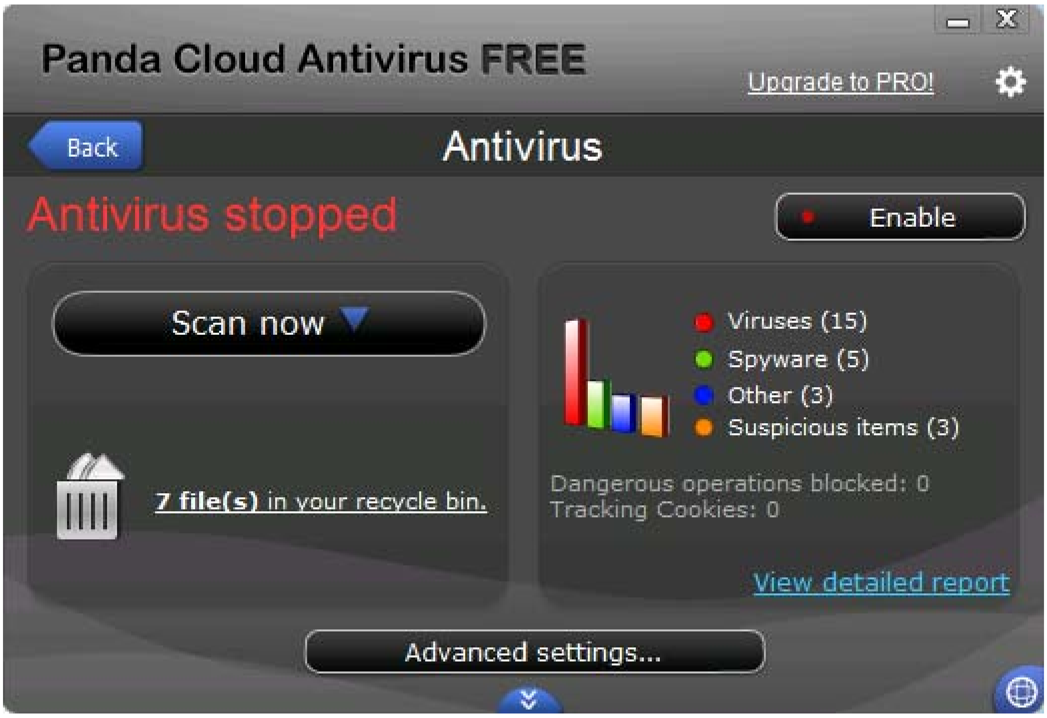
Program interface

The main functionality of the program is located in a horizontal panel in the top half of the window:



Scanned/min: 0

The shield symbol on the left is the status display. If all is well, it is a turquoise colour, and displays the text "Secure". If the real-time protection is disabled, it turns red, and displays the word "Stopped"; we feel this is not the clearest warning we have seen on an antivirus program, as it could be interpreted as meaning "The scan has stopped", which would not be so critical. Clicking anywhere on the panel shown above opens a more detailed information/configuration page, which clearly states "Antivirus stopped" in red, with a button marked Enable (which changes to "Disable" when real-time protection is on):



Antivirus stopped

7 file(s) in your recycle bin.

- Viruses (15)
- Spyware (5)
- Other (3)
- Suspicious items (3)

Dangerous operations blocked: 0
Tracking Cookies: 0

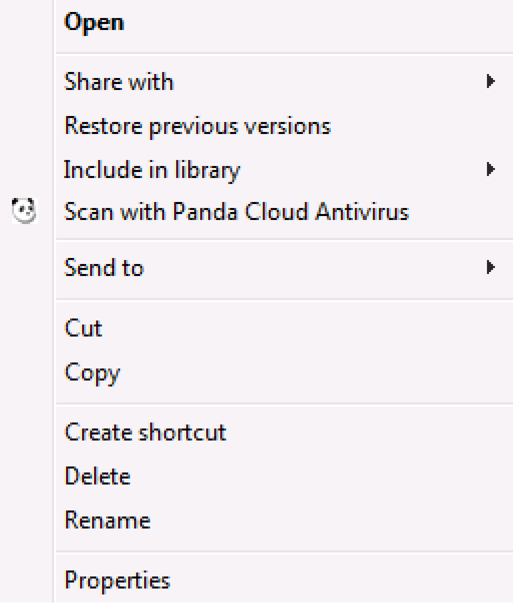
The same page provides a big button marked "Scan now", which is actually a scan menu, with the options Optimized Scan (quick scan), Full Scan, and Scan Other Items; we found the latter slightly confusing, but it is in fact a custom scan option, allowing drives and folders to be selected for scanning.

The item named "recycle bin" is actually the quarantine. We find the name to be rather inappropriate, and potentially confusing for non-experts, who may get it mixed up with the Windows Recycle Bin.

As its name suggests, Panda Cloud Antivirus uses cloud-based signatures, and so there is no Update button. As it is a free program, there is also no subscription information.

The help functions are available from the cogwheel symbol in the top right-hand corner of the window, which is visible regardless of which page is shown in the main panel.

Panda Cloud Antivirus Free integrates itself into Windows Explorer's context menu with a scan entry:



Default configuration

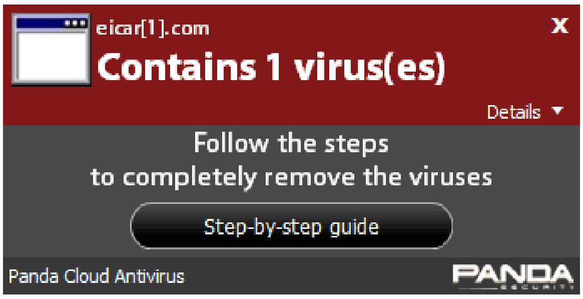
Non-administrator access

When we logged on to our test PC with a non-administrator account, it was possible to disable the real-time protection just as easily as with an administrator account, which we do not consider to be ideal.

Scanning and malware discovery

A scheduled scan is not available in Panda Cloud Antivirus Free. Not surprisingly for a cloud-based program, there is also no means of running a boot-time scan.

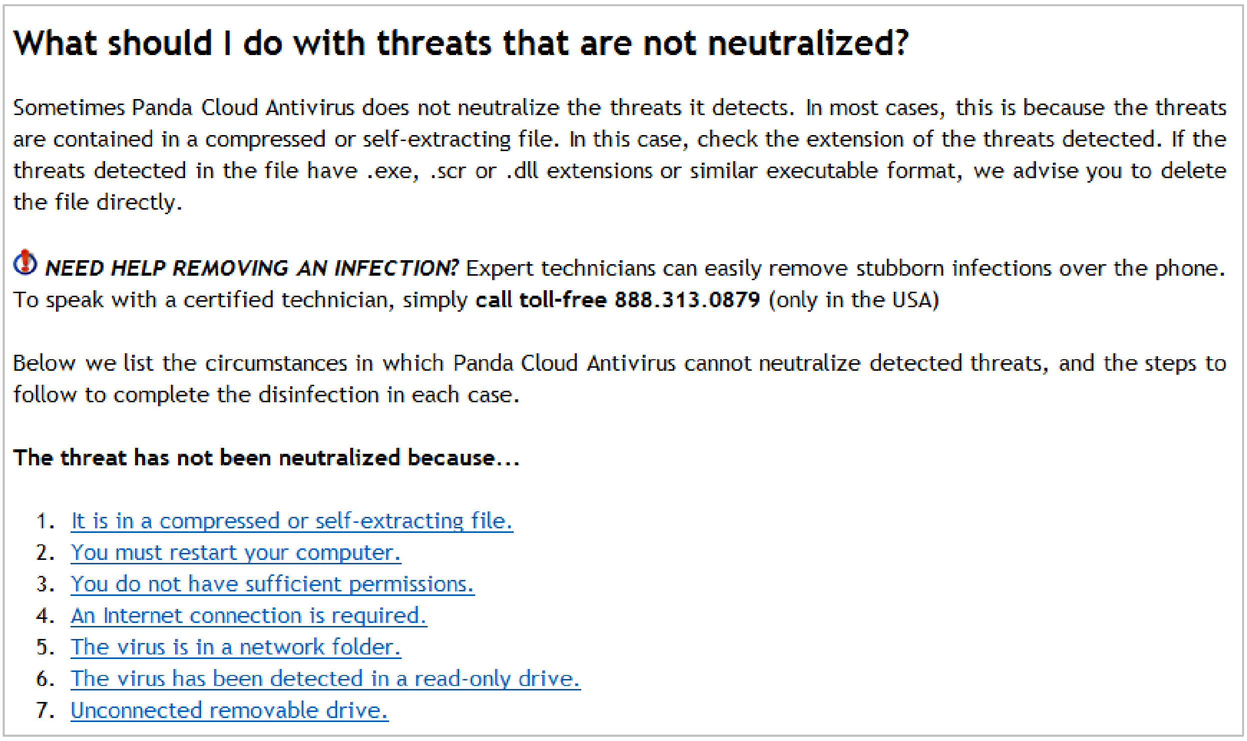
When we attempted to download the EICAR test file, Panda displayed the following alert:


eicar[1].com

Contains 1 virus(es)

Follow the steps to completely remove the viruses

We were rather surprised to see that a step-by-step guide should be necessary to block the download of a (supposedly) malicious file, but clicked on the "Step-by-step guide" button anyway, as it appeared to be necessary. This then opened a page from the online help service, shown below:



What should I do with threats that are not neutralized?

Sometimes Panda Cloud Antivirus does not neutralize the threats it detects. In most cases, this is because the threats are contained in a compressed or self-extracting file. In this case, check the extension of the threats detected. If the threats detected in the file have .exe, .scr or .dll extensions or similar executable format, we advise you to delete the file directly.

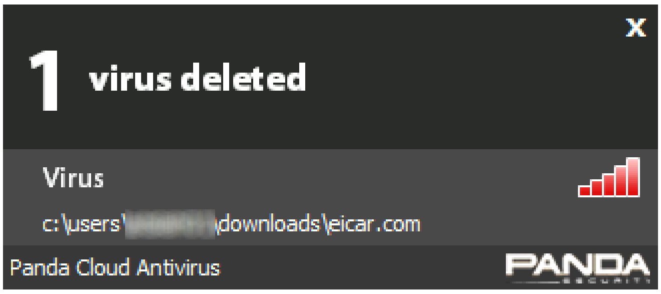
NEED HELP REMOVING AN INFECTION? Expert technicians can easily remove stubborn infections over the phone. To speak with a certified technician, simply **call toll-free 888.313.0879** (only in the USA)

Below we list the circumstances in which Panda Cloud Antivirus cannot neutralize detected threats, and the steps to follow to complete the disinfection in each case.

The threat has not been neutralized because...

1. It is in a compressed or self-extracting file.
2. You must restart your computer.
3. You do not have sufficient permissions.
4. An Internet connection is required.
5. The virus is in a network folder.
6. The virus has been detected in a read-only drive.
7. Unconnected removable drive.

The page can hardly be described as a step-by-step guide, as it merely lists a number of possible courses of action to try. We imagine that many non-expert users would be worried by this, and assume that the only way to protect their computer would be to systematically go through all 7 of the scenarios listed. We note that we downloaded the simple version of the EICAR test file, not any of the zipped versions, so the first item in the list ("It is in a compressed or self-extracting file") is no more applicable than most of the other scenarios. Safe in the knowledge that the EICAR test file posed no threat to our test PC, we closed the original dialog box, and were astonished to see the following message box had been hidden underneath, and stated very simply that the "virus" had been deleted:



1 virus deleted

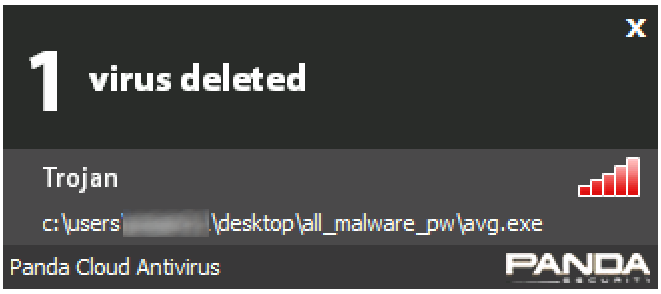
Virus

c:\users\[redacted]\downloads\eicar.com

Panda Cloud Antivirus

We are baffled as to why Panda have deemed fit to display the first message box, with its instruction to follow a complicated and irrelevant "step-by-step guide", when the second message box, hidden underneath, makes perfectly clear that the threat has already been deleted. We would urge Panda to remove the confusing first message box.

When malware was discovered locally on our PC by Panda's real-time protection, the following message was displayed:



1 virus deleted

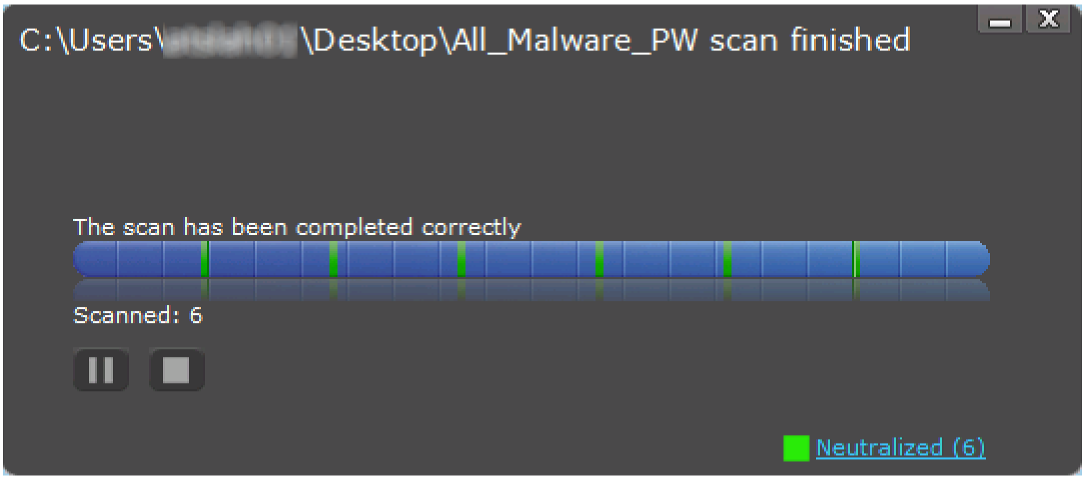
Trojan

c:\users\[redacted]\desktop\all_malware_pw\avg.exe

Panda Cloud Antivirus

This makes perfectly clear that the malware has been deleted.

When we scanned our malware folder from the console or context menu, Panda displayed the following report, stating that all the threats had been neutralised:



C:\Users\[redacted]\Desktop\All_Malware_PW scan finished

The scan has been completed correctly

Scanned: 6

🟩 Neutralized (6)

Scanning without cloud access

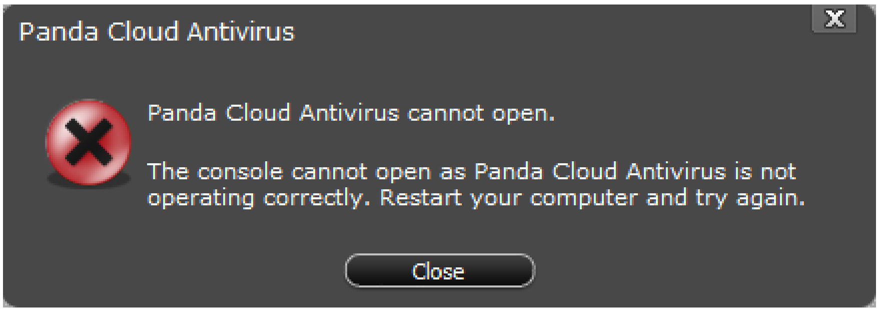
As Panda Cloud Antivirus Free obviously relies significantly on its cloud service for malware detection, we performed a simple test to get an idea of how it behaves when offline, i.e. when the computer does not have an Internet connection, and so the program cannot access its database on the server. This simulates a situation where a laptop user connects a USB flash drive containing malware to their computer when offline. The test should not be seen as an effective malware detection test, as it used only 6 Trojans and the EICAR test file (although the results are supported by the vastly more extensive lab tests carried out by AV-Comparatives). The purpose is to see whether the program warns that its detection capabilities are reduced when there is no access to the cloud.

The test was done on a newly installed system which had not been used for malware testing previously, to exclude the possibility that Panda Cloud Antivirus Free had locally cached signatures of malware it had already detected with a cloud connection. As with our other scanning tests, Windows Defender was disabled.

To run the test, we disabled the network adapter on our test PC, restarted the computer, and checked that there was no network/Internet access. We next opened Panda Cloud Antivirus Free, and checked whether the program displayed any warning to the effect that it was offline, which it did not. We then unzipped and scanned our folder of malware, to see if the program was able to identify any of the items without cloud access. We found that Panda managed to identify and quarantine 4 out of the 6 Trojans in the folder (with cloud access it detected the two remaining items as well). Evidently Panda Cloud Antivirus Free is by no means entirely dependent on the cloud for malware identification; however, there was no warning before, during or after the scan that the program was offline.

Safe Mode

When we started our test PC in Safe Mode with Networking and attempted to open Panda Cloud Antivirus Free, the following message was displayed:


Panda Cloud Antivirus

Panda Cloud Antivirus cannot open.

The console cannot open as Panda Cloud Antivirus is not operating correctly. Restart your computer and try again.

We also found that the scan entry in Windows Explorer’s context menu had been removed, and so we were unable to run any sort of scan.

Help and documentation

Not surprisingly for a cloud-based program, Panda Cloud Antivirus Free uses an online help function. It is laid out like a traditional Windows Help file, with a tree of topics in a left-hand panel, and a main panel on the right to show the details of the topic selected. We note that the Free edition of the program uses the same help function as the Pro; we found Firewall Settings amongst the items in the tree on the left-hand side, even though the Free edition does not include a firewall. As it is not possible to run a scheduled scan with the program, we just searched for “scan exclusions”; whilst the instructions we found for setting exclusions were clear and simple, there are no directions for finding the relevant page of the settings, which we feel rather misses the point of a help function.

There is also an online forum, accessible by clicking on the cogwheel symbol in the top right-hand corner of the program window, and then clicking Online Tech Support on the resulting menu. This enables users to submit queries or search existing answers. We were unable to find a manual for Panda Cloud Antivirus, either Free or Pro.

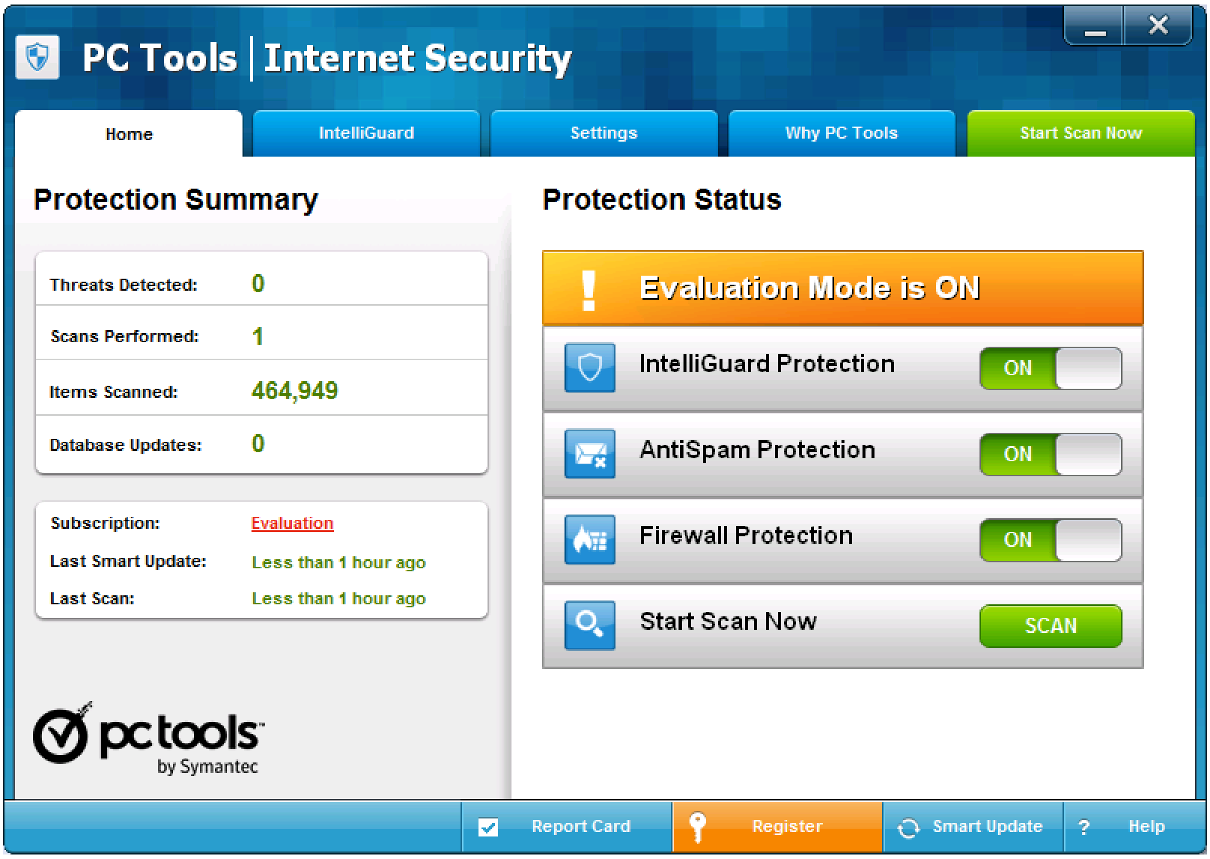
In summary, we feel that the help functions for Panda Cloud Antivirus Free could be improved.

Verdict

We would say that the user interface of Panda Cloud Antivirus Free is largely fine for reasonably confident users who are not afraid to explore a little, although for non-experts it is not quite as clear as it might be. We note that despite being essentially a cloud-based program, Cloud Antivirus Free is still able to detect some malware when offline.

Warning messages and default actions on malware discovery are largely good, with the one major exception of the potentially very confusing alert that popped up when downloading the EICAR test file. We would strongly recommend that Panda remove this from the program. We also found the help functions rather disappointing and suggest that they could be improved.

PC Tools Internet Security 9.1



Protection Summary

Threats Detected:	0
Scans Performed:	1
Items Scanned:	464,949
Database Updates:	0

Subscription:	Evaluation
Last Smart Update:	Less than 1 hour ago
Last Scan:	Less than 1 hour ago

Protection Status

Evaluation Mode is ON

IntelliGuard Protection	ON
AntiSpam Protection	ON
Firewall Protection	ON
Start Scan Now	SCAN

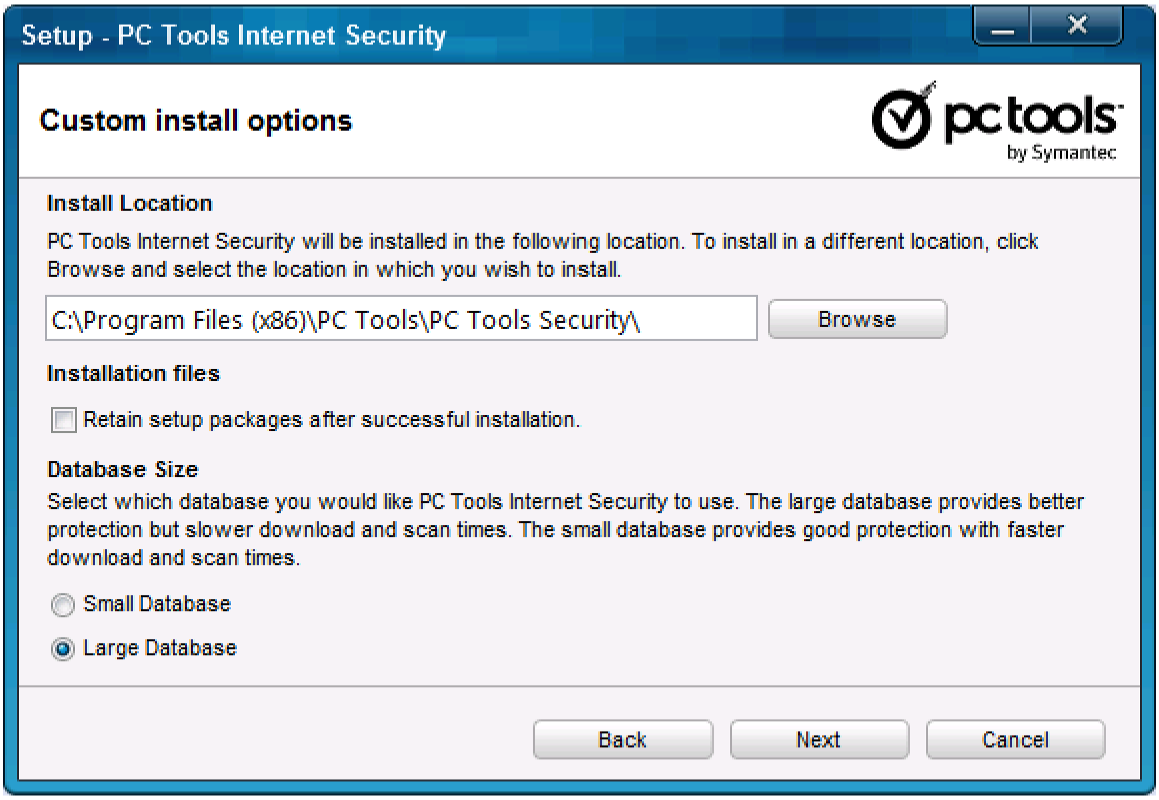
Components

PC Tools Internet Security 9.1 comprises an antimalware component with email scanning, antispam component, and firewall.

Installation

We installed the trial version of PC Tools Internet Security 9.1, which is supplied as a 4 MB downloader file. The installation wizard starts by presenting the licence agreement to be accepted, then moves on to the choices “Enter a licence key”, “Buy now”, and, rather confusingly we thought, “Try a free scan”. The latter option does install the full program, however. There is also a choice of Easy Install or Custom Install; we chose the latter.

The options available in the Custom Install are folder location, whether to retain the setup files after installation, and, unusually, database size:



Setup - PC Tools Internet Security

Custom install options

Install Location

PC Tools Internet Security will be installed in the following location. To install in a different location, click Browse and select the location in which you wish to install.

C:\Program Files (x86)\PC Tools\PC Tools Security\

Installation files

☐ Retain setup packages after successful installation.

Database Size

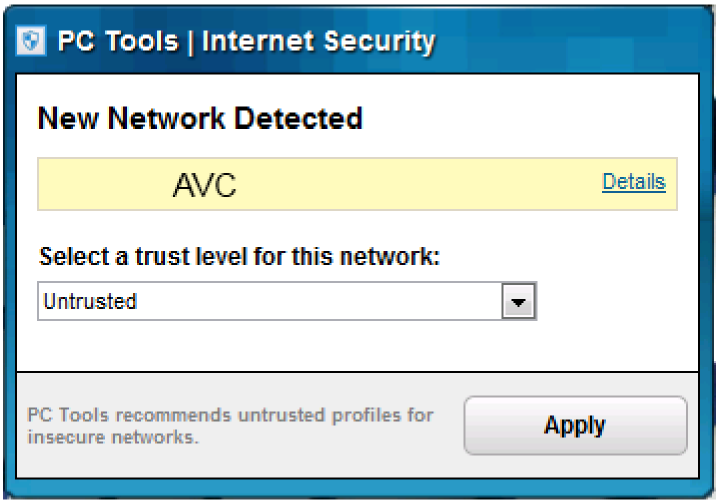
Select which database you would like PC Tools Internet Security to use. The large database provides better protection but slower download and scan times. The small database provides good protection with faster download and scan times.

○ Small Database

● Large Database

Having made choices for the three items on this page, the user then only needs to click Next, and installation begins. There are no other options such as choice of components or languages. The wizard displays some tips and information about the suite during the download/installation process. A reboot was not required.

At the end of the setup process, PC Tools' installer asks the user to say if the current network is Trusted or Untrusted, i.e. private or public:



PC Tools | Internet Security

New Network Detected

AVC

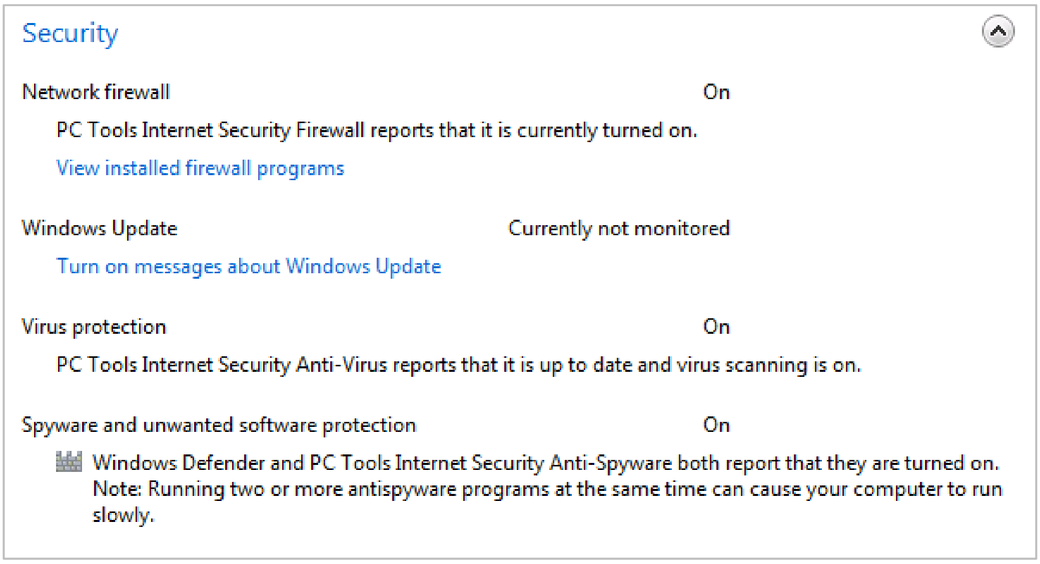
Select a trust level for this network:

Untrusted

PC Tools recommends untrusted profiles for insecure networks.

We chose Trusted, in keeping with the test PC's current Windows settings.

PC Tools Internet Security registers itself in Windows Action Center as an antivirus and antispyware program and firewall. Windows Firewall is disabled, Windows Defender is not.



Security

Network firewall On

PC Tools Internet Security Firewall reports that it is currently turned on.

View installed firewall programs

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

PC Tools Internet Security Anti-Virus reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

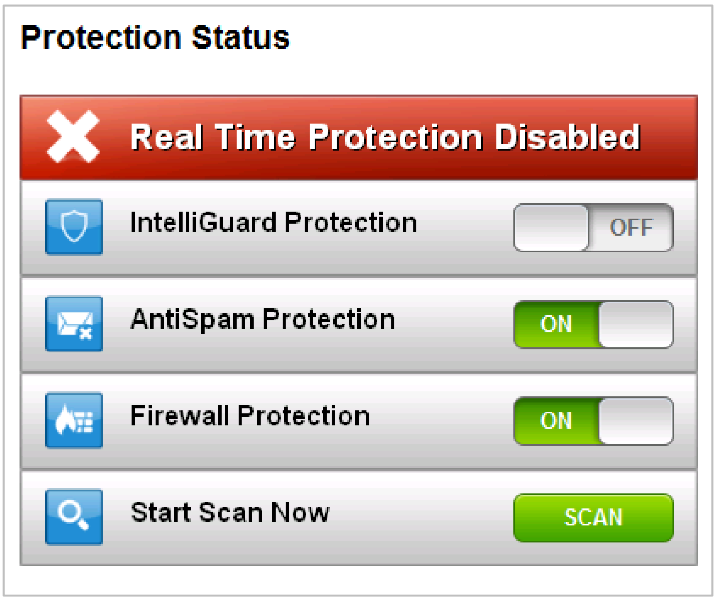
Windows Defender and PC Tools Internet Security Anti-Spyware both report that they are turned on. Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

If the suite’s real-time protection or firewall are disabled, Windows Action Center immediately shows an alert.

PC Tools’ uninstaller has no options at all, it can only be used to remove the product completely. It does allow the user to keep existing settings (if desired), in the event that the product is to be reinstalled later.

Program interface

The home page of PC Tools Internet Security is divided into two main panes: a slightly smaller left-hand pane, which shows licence and update information and scanning statistics, and a larger right-hand pane, showing the major protection components, with an on/off button for each, and overall protection status. Please note that in the trial version, the overall protection status bar displays the message "Evaluation Mode is ON"; with a subscription, this would show "Balanced Mode is ON". If real-time protection is disabled, the overall status display changes to show this:

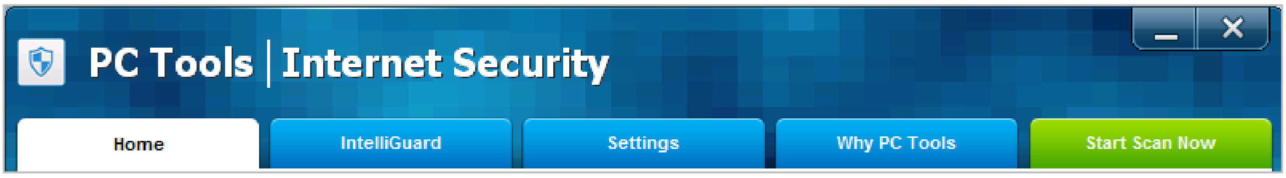


There is no "Fix All" button, but this is quite unnecessary, as the IntelliGuard Protection button below clearly shows that it is off, and easily enables it to be switched back on.

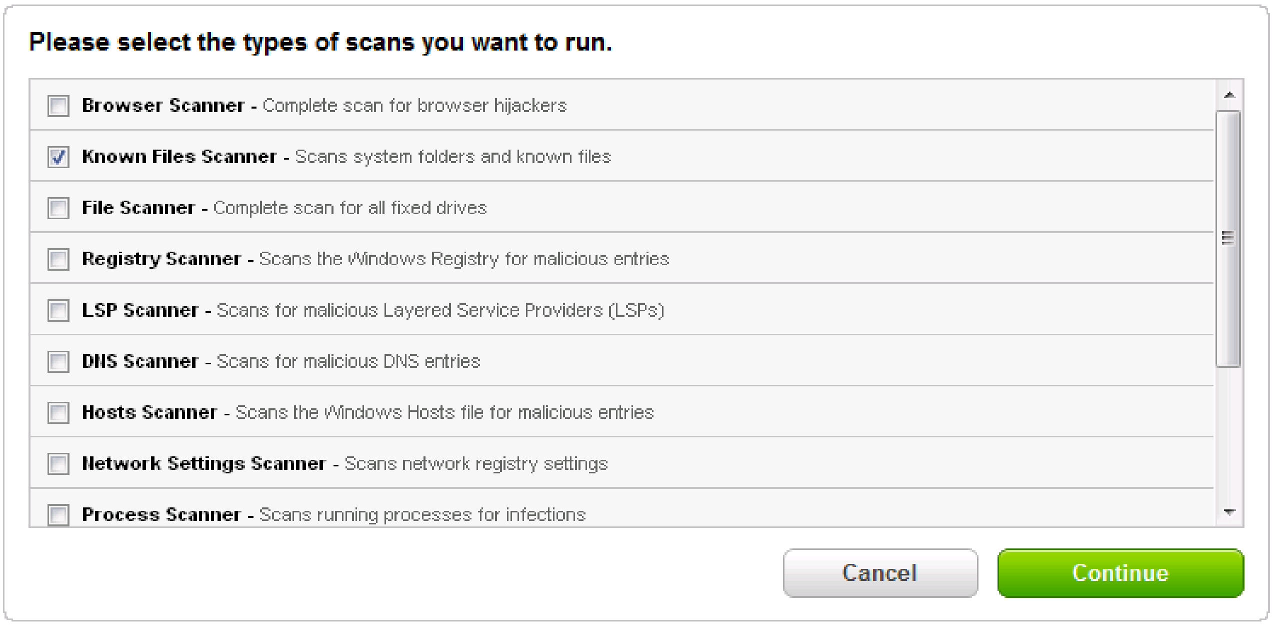
We note that shortly after installation a brief scan was run automatically, lasting just under three minutes. We observed that the Protection Summary section of the home page then displayed "Items Scanned: 464,949", which would appear to be an extraordinary achievement within the space of 175 seconds; it amounts to 2,656 items scanned per second.

Virus signatures can be updated using the Smart Update button at the bottom of the window. We were surprised to see that using this brings up a Windows User Account Control prompt; please see the note on Non-Administrator Access below.

A row of tabs along the top of the window enables access to other functions and settings:



IntelliGuard allows configuration of the real-time protection; Settings enables configuration of the other components; Start Scan Now, not surprisingly, provides access to the scan functions. There are three major scan options, namely IntelliScan (quick scan), Full Scan, and Custom Scan. Although the description of Custom Scan states “Specify folders to scan”, we were unable to choose drives or folders with this. The available choices related to specific problems to scan for, such as malicious registry entries or “malicious Layered Service Providers”:



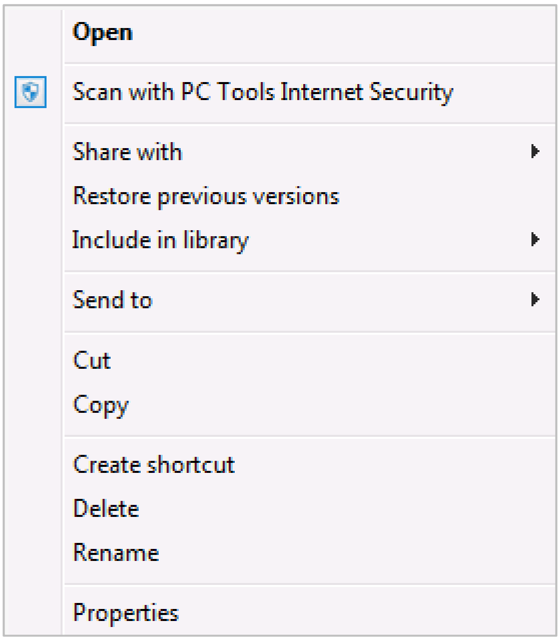
Please select the types of scans you want to run.

- □ **Browser Scanner** - Complete scan for browser hijackers
- ☑ **Known Files Scanner** - Scans system folders and known files
- □ **File Scanner** - Complete scan for all fixed drives
- □ **Registry Scanner** - Scans the Windows Registry for malicious entries
- □ **LSP Scanner** - Scans for malicious Layered Service Providers (LSPs)
- □ **DNS Scanner** - Scans for malicious DNS entries
- □ **Hosts Scanner** - Scans the Windows Hosts file for malicious entries
- □ **Network Settings Scanner** - Scans network registry settings
- □ **Process Scanner** - Scans running processes for infections

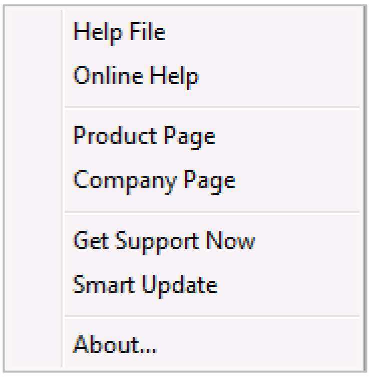
We suggest that inexperienced users would be entirely baffled by such a selection, and even advanced users might wonder why it is necessary to specify items in so much detail.

We did not find any means of running a boot-time scan.

PC Tools Internet Security integrates itself into Windows Explorer by means of a single entry in the context menu, “Scan with PC Tools Internet Security”.



The suite's help functions can be easily accessed by clicking the Help Button in the bottom right-hand corner, which displays the following menu:



We found the overall design of PC Tools Internet Security's program window to be clear and effective, providing the user with essential information and easy access to important functions.

Default configuration

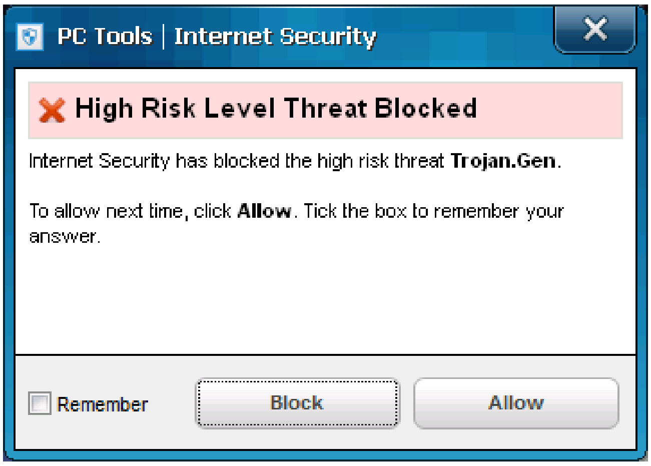
Non-administrator access

When we logged on to our test PC using a non-administrator account, we found we could still disable major components of the suite, such as the firewall and real-time protection, without any password being required. We feel that this is not ideal, especially for users such as parents who set up non-administrator accounts for their children in order to prevent major system changes being made. Trying to update the malware signatures using the Smart Update button brought up a UAC prompt demanding an administrator password; without this, the program cannot be updated. We can only say that we are baffled as to why PC Tools allow non-administrators to disable protection, but not update signatures.

Scanning and malware discovery

Both a full scan and an Intelli-Scan (quick scan of most important areas) are set up by default. They can easily be edited by clicking on Settings, Scheduled Tasks.

On discovering malware locally, PC Tools Internet Security displayed the following dialog box:



PC Tools | Internet Security

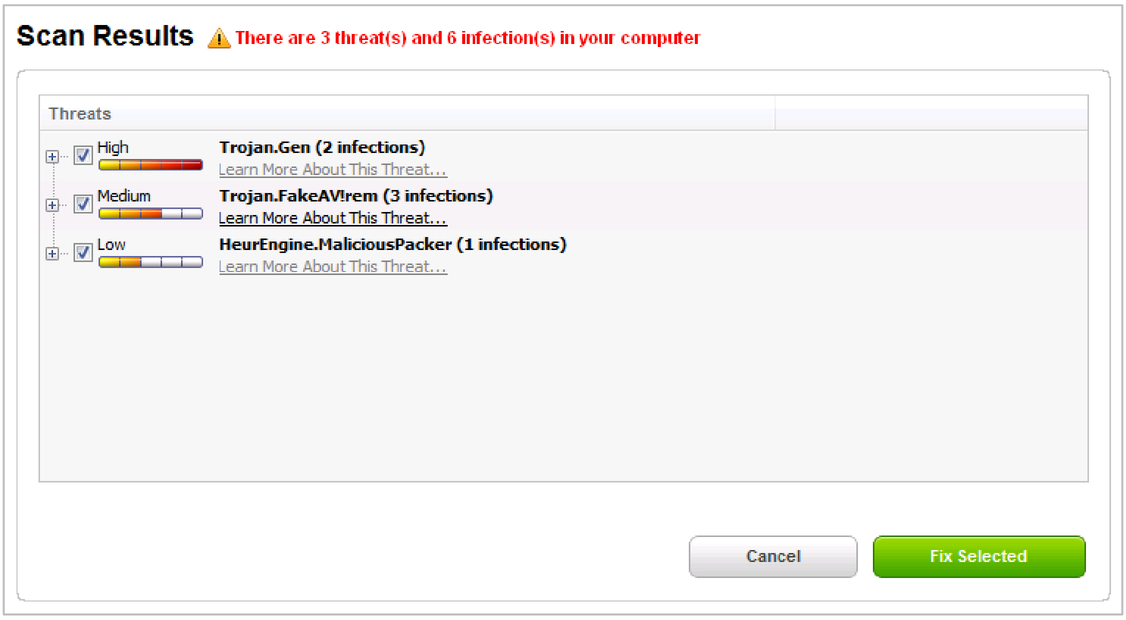
High Risk Level Threat Blocked

Internet Security has blocked the high risk threat **Trojan.Gen**.

To allow next time, click **Allow**. Tick the box to remember your answer.

We found that clicking Block would prevent a malware file from executing, although it was not deleted or quarantined. Clicking Allow permitted the malicious program to execute; we found this rather alarming, considering that PC Tools describes the program as "High Risk Level". An accidental click, whether caused by lack of thought or over-sensitive touchpad, could potentially have unintended consequences.

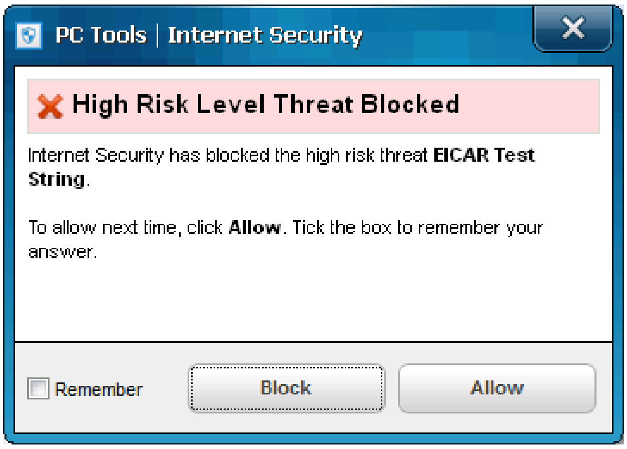
As mentioned above, we were unable to run a custom scan of the folder containing our malware samples from the console, as individual folders cannot be selected. When we scanned the folder using Windows Explorer's context menu, the following page was displayed in the main program window, allowing us to remove the malware found:



Scan Results There are 3 threat(s) and 6 infection(s) in your computer

Threats	
☑ High	**Trojan.Gen (2 infections)** Learn More About This Threat...
☑ Medium	**Trojan.FakeAV!rem (3 infections)** Learn More About This Threat...
☑ Low	**HeurEngine.MaliciousPacker (1 infections)** Learn More About This Threat...

When we attempted to download the EICAR test file, PC Tools presented the following dialog box:

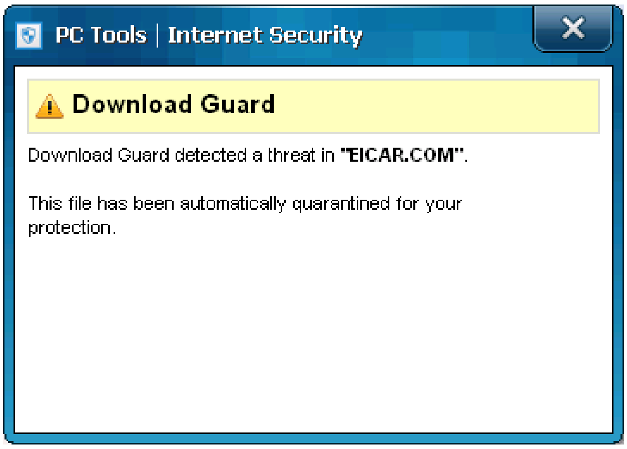


High Risk Level Threat Blocked

Internet Security has blocked the high risk threat **EICAR Test String**.

To allow next time, click **Allow**. Tick the box to remember your answer.

If we clicked Allow, we found that the file was downloaded, remained visible for a few seconds, and was then moved into Quarantine by a different process of the suite:



Download Guard

Download Guard detected a threat in **"EICAR.COM"**.

This file has been automatically quarantined for your protection.

Whilst this would have protected the PC from a real threat, we wondered why we had been given the choice of downloading the file at all.

Inbound firewall settings

Having defined our PC's network as Trusted during installation, we found that we were able to ping it, access the file share and use Remote Desktop without any restriction. Changing the network type to Untrusted in the Firewall Settings (very quickly and easily done) then blocked all three types of access completely.

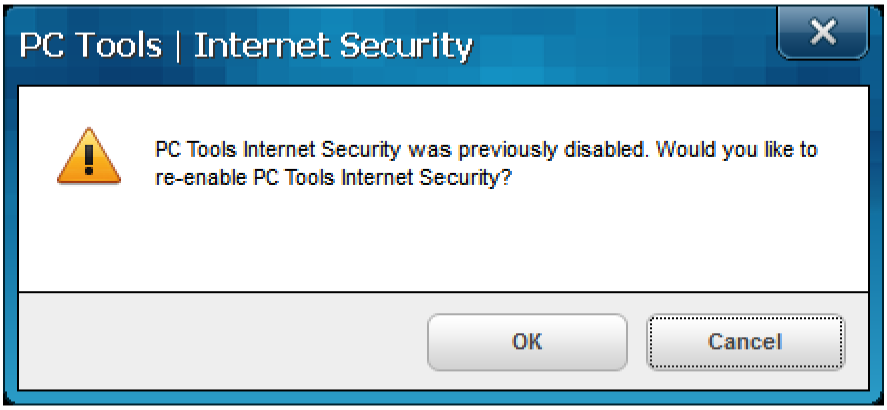
Connecting to a different network causes PC Tools Internet Security to ask the user again whether the network should be trusted or not. However, changing the network type from Work to Public in Windows' Network and Sharing Center (as if the user had made a mistake when initially selecting this) did not change the network type in PC Tools Internet Security, so the user would have to change this additionally to ensure appropriate protection.

Outbound firewall/application control

When we ran our firewall testing program, PC Tools Internet Security allowed it to access the Internet without query, despite the fact that application control is switched on by default. We conclude that the suite had correctly identified the program as being harmless.

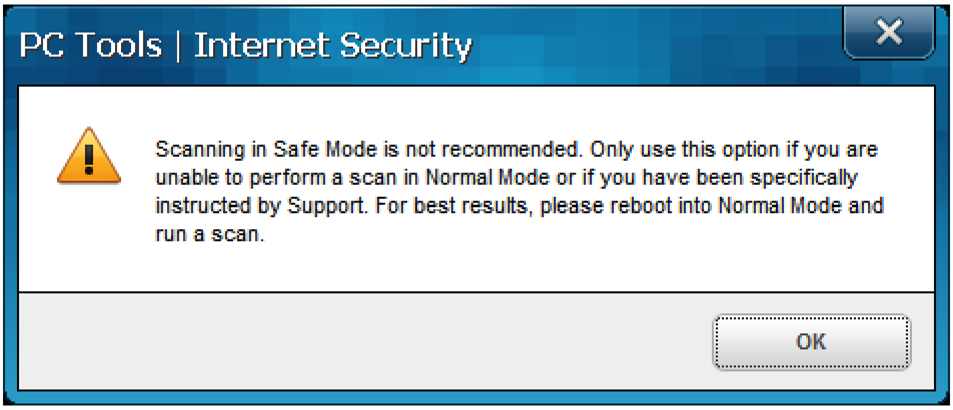
Safe Mode

When our test PC was started in Safe Mode with Networking, we attempted to run a context-menu scan on our folder of malware, but were confronted by an error message. However, we were able to start the program by clicking on its icon and confirming the action:



PC Tools Internet Security was previously disabled. Would you like to re-enable PC Tools Internet Security?

We were then able to run a context-menu scan on our malware folder, after confirming another message box:



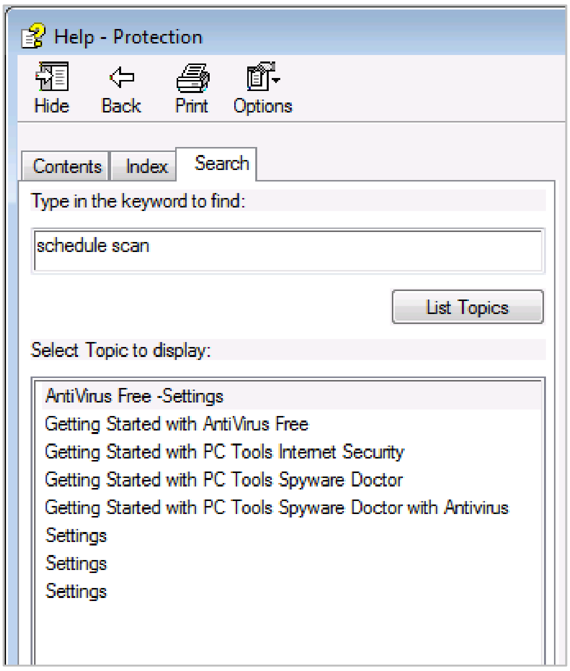
Scanning in Safe Mode is not recommended. Only use this option if you are unable to perform a scan in Normal Mode or if you have been specifically instructed by Support. For best results, please reboot into Normal Mode and run a scan.

As in normal mode, the program presented us with a list of the items it had found, and allowed us to remove them by clicking “Fix Selected”.

Help and documentation

Before describing the help features of the suite, we must point out that one of our standard queries used with all products in this review is how to set scanning exclusions, i.e. define files or folders that should be excluded from antimalware scans. We were unable to find any means of actually doing this in PC Tools Internet Security; File Exclusions in Scan Settings allows specific file types, defined by file extension, to be excluded from scanning, but does not allow the user to define individual files or folders in specific locations. As a consequence of this, there was no sense in trying to find instructions for scan exclusions in the help services.

The Help button in the bottom right-hand corner of the program window provides quick and easy access to both local and online help functions. In the local help, we were quickly able to find clear and simple instructions for setting up a scheduled scan. We did note, however, that the Help file evidently contains instructions for other PC Tools products as well, as the screenshot below illustrates:



Type in the keyword to find:

schedule scan

Select Topic to display:

AntiVirus Free -Settings
Getting Started with AntiVirus Free
Getting Started with PC Tools Internet Security
Getting Started with PC Tools Spyware Doctor
Getting Started with PC Tools Spyware Doctor with Antivirus
Settings
Settings
Settings

We also observer that there are three different entries all called “Settings”, without any indication as to which product each one belongs to; we do not feel that this is consistent with a professionally produced product.

Searching the online help service produced an almost identical list of entries, the only difference being that the 3 Settings entries were labelled with the names of the products they referred to. The text of the instructions provided for scheduling a scan was identical to that found in the local help service, without any additions such as illustrations, making the online help service appear effectively redundant.

Searching for a manual for PC Tools Internet Security on the manufacturer’s website yielded a link to “User Guides”, which sounded promising, but turned out to be the online help service with a different name. We conclude that there is no separate manual as such.

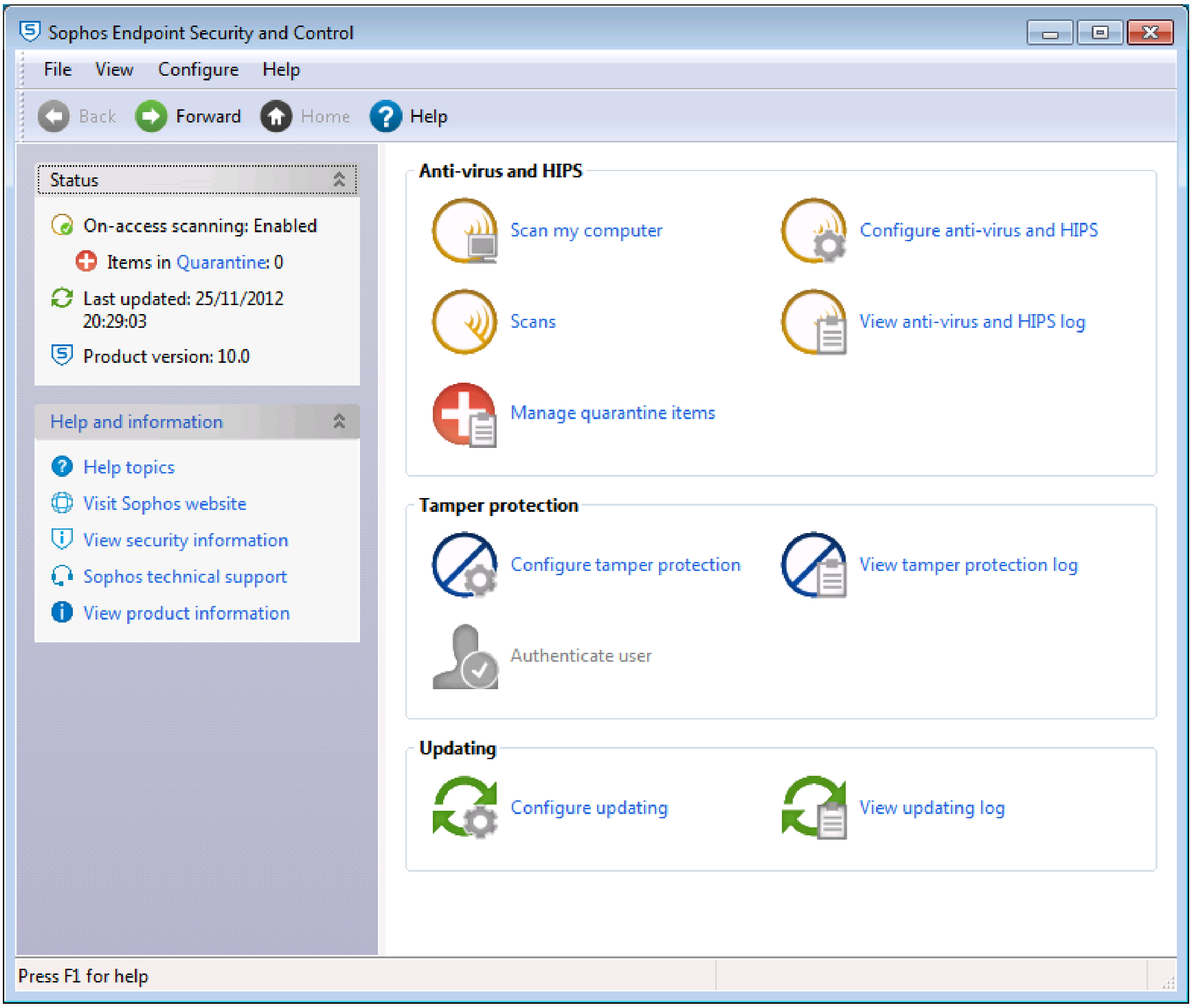
Compared to the extensive online knowledge bases and comprehensive manuals produced by some manufacturer’s, we can only describe the help functions for PC Tools Internet Security as “simple”.

Verdict

PC Tools Internet Security is in some ways an unproblematic suite with a simple layout. Installation is simple, all the major functions are easily accessible from the home page, and finding one's way around the interface is very straightforward. We also note that warnings from the suite itself and from Windows 7's Action Center are now optimal, much improved on last year's version. Unfortunately, we feel obliged to mention two issues which we would regard as serious. We found that it is possible to run a malicious program, which the suite itself defines as a "High Risk Level Threat", simply by clicking "Allow" on the PC Tools dialog box. We also find it bizarre that a user without administrator rights can completely disable the real-time protection and firewall without any sort of query or hindrance, but cannot update the virus signatures without entering administrator credentials. There are also a few less serious issues, such as the baffling options available for a custom scan, and a very limited help function.

Whilst we feel that an experienced, confident user would be able to work around the suite's shortcomings, we do not feel that we can recommend it for non-experts or family use.

Sophos Endpoint Protection 10.0



Nature of the program

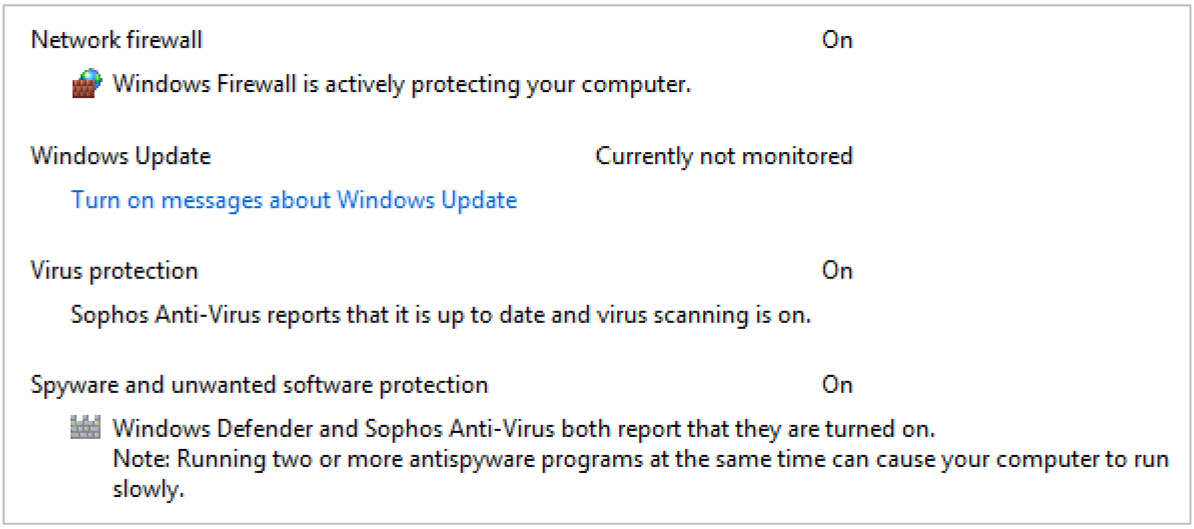
Please note that Sophos Endpoint Protection is designed for use in a managed business environment, meaning that its interface and features cannot be directly compared to those of consumer Internet security suites.

Components

Sophos Endpoint Protection consists of an antimalware component (Sophos Anti-Virus) and optional firewall.

Installation

We installed Sophos Endpoint Protection from a 98 MB full installer, available on the Sophos website as a trial version. The setup wizard starts by unpacking the installation files into a directory on the local hard drive, which can be changed. There is then a licence agreement to accept, a choice of installation directory, entry of update credentials (equivalent to licence key), and the option to install the Sophos firewall. As this is not selected by default, we chose not to install it, in line with our standard installation practice. There is an option to remove any existing security software, and installation then begins.



Network firewall On

Windows Firewall is actively protecting your computer.

Windows Update Currently not monitored

Turn on messages about Windows Update

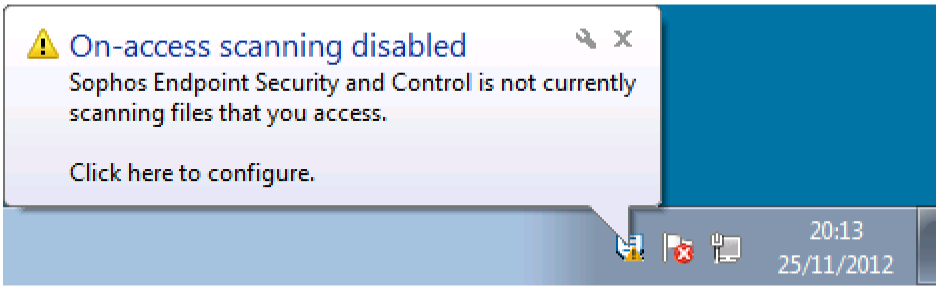
Virus protection On

Sophos Anti-Virus reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

Windows Defender and Sophos Anti-Virus both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

Sophos Endpoint Protection registers itself in Windows Action Center as an antivirus and antispyware program. Neither Windows Defender nor Windows Firewall is disabled. When we disabled Sophos' real-time protection, Action Center displayed its standard alert. Sophos Endpoint Protection additionally displayed its own alert:



On-access scanning disabled

Sophos Endpoint Security and Control is not currently scanning files that you access.

Click here to configure.

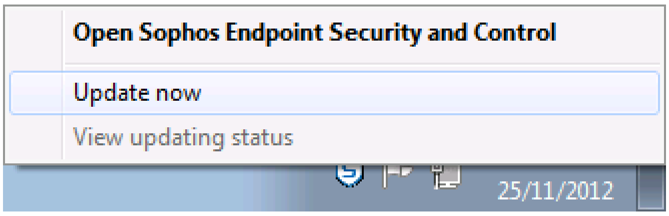
Sophos' uninstaller has no options other than complete removal.

Program interface

The main program window consists of a narrower left-hand panel with boxes for status information and help items. A larger right-hand pane displays links for configuring components and functions. This includes "Scan my computer", which runs a full scan, and "Scans" which allows custom scans to be configured and scheduled.

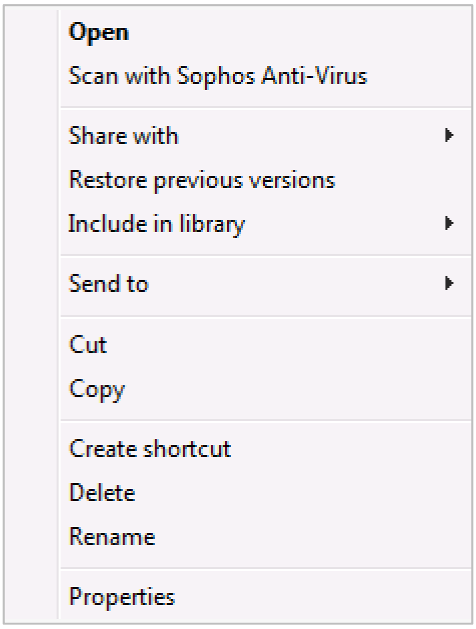
The status display is limited to a single entry in the Status box in the top left-hand corner, which simply states whether the real-time protection is active. There is no obvious link to re-enable it, but this is less important in a business product managed from a central console.

Updating the malware signatures is done by right-clicking the System Tray icon and clicking Update Now:



Subscription information is not displayed, but again this is not necessary for a centrally managed business product. The local help function can be opened by clicking Help on the toolbar at the top of the program, while web-based support features can be accessed from the Help and Information box in the left-hand panel.

Sophos integrates itself into Windows Explorer's context menu with a scan entry:



Default configuration

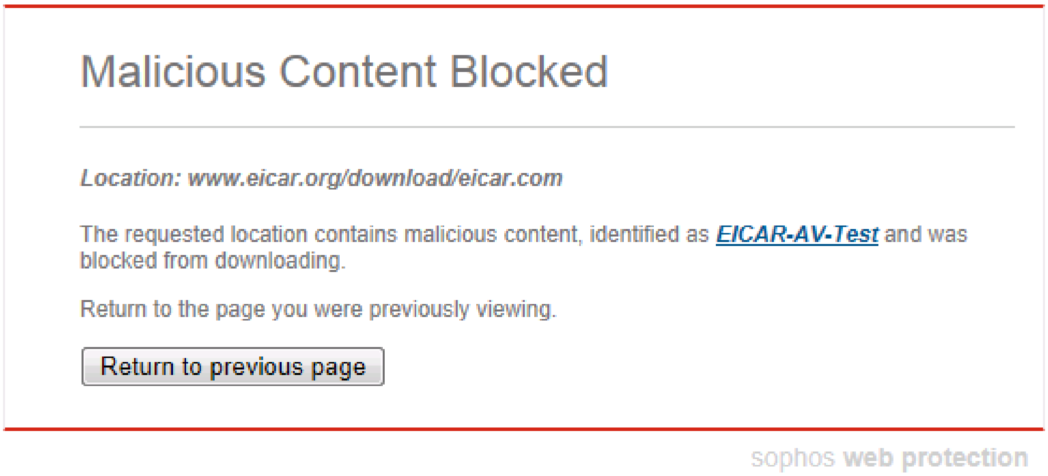
Non-administrator access

When we logged on to our test PC with a non-administrator account, we found that most of the antivirus configuration options, including those for real-time protection, had been disabled. This is exactly what we would expect from a product made for business use.

Scanning and malware discovery

A scheduled scan is not set by default, but can be configured easily from the Scans button on the home page. We could not find a means of running a boot-time scan.

When we attempted to download the EICAR test file, Sophos blocked the webpage with the following message:



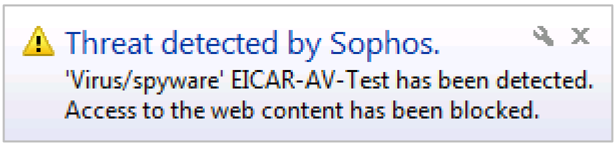
Malicious Content Blocked

Location: www.eicar.org/download/eicar.com

The requested location contains malicious content, identified as ***EICAR-AV-Test*** and was blocked from downloading.

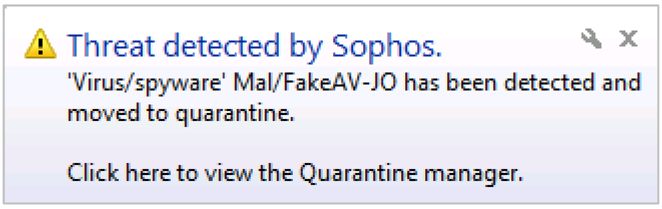
Return to the page you were previously viewing.

Additionally, an alert was shown by Sophos' System Tray icon:



Threat detected by Sophos.
'Virus/spyware' EICAR-AV-Test has been detected.
Access to the web content has been blocked.

When malware was detected locally on the PC by Sophos' real-time protection, access to the file was blocked, and the following alert shown by the System Tray icon:

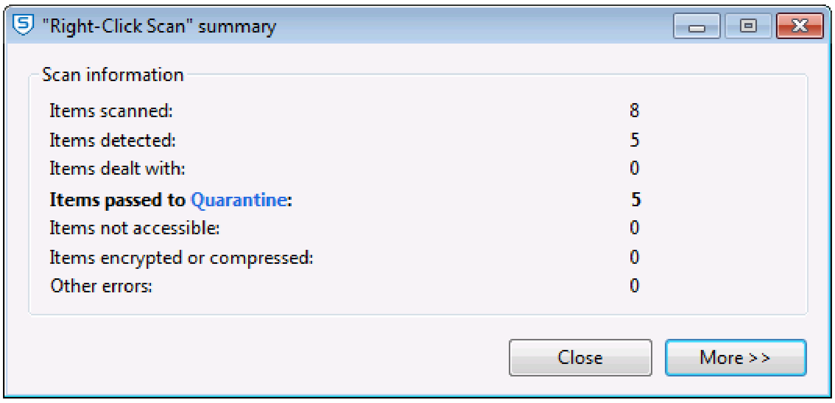


Threat detected by Sophos.
'Virus/spyware' Mal/FakeAV-JO has been detected and moved to quarantine.

Click here to view the Quarantine manager.

We note that while the malware file was completely disabled, it was not actually removed from its original location until the computer was rebooted. We feel this might prove confusing for some users.

When we ran a custom or context-menu scan, Sophos displayed the following message box:



"Right-Click Scan" summary

Scan information

Items scanned:	8
Items detected:	5
Items dealt with:	0
Items passed to Quarantine:	**5**
Items not accessible:	0
Items encrypted or compressed:	0
Other errors:	0

Clicking on More displays a list of the malware items found and quarantined. In this case, we found that the malware items had been removed from their original location.

Safe Mode

When we started our test PC in Safe Mode with Networking, we were unable to run an update, as the System Tray icon (normally used to do this) did not appear. However, we found that a context-menu scan ran as normal.

Help and documentation

The local help function is accessed by clicking the Help button on the toolbar of the main window. It has a traditional Windows Help window, with a list of topics in a left-hand pane, details of which are shown in a larger right-hand pane. There is a search function, and we were quickly able to find clear and simple answers to our two standard queries.

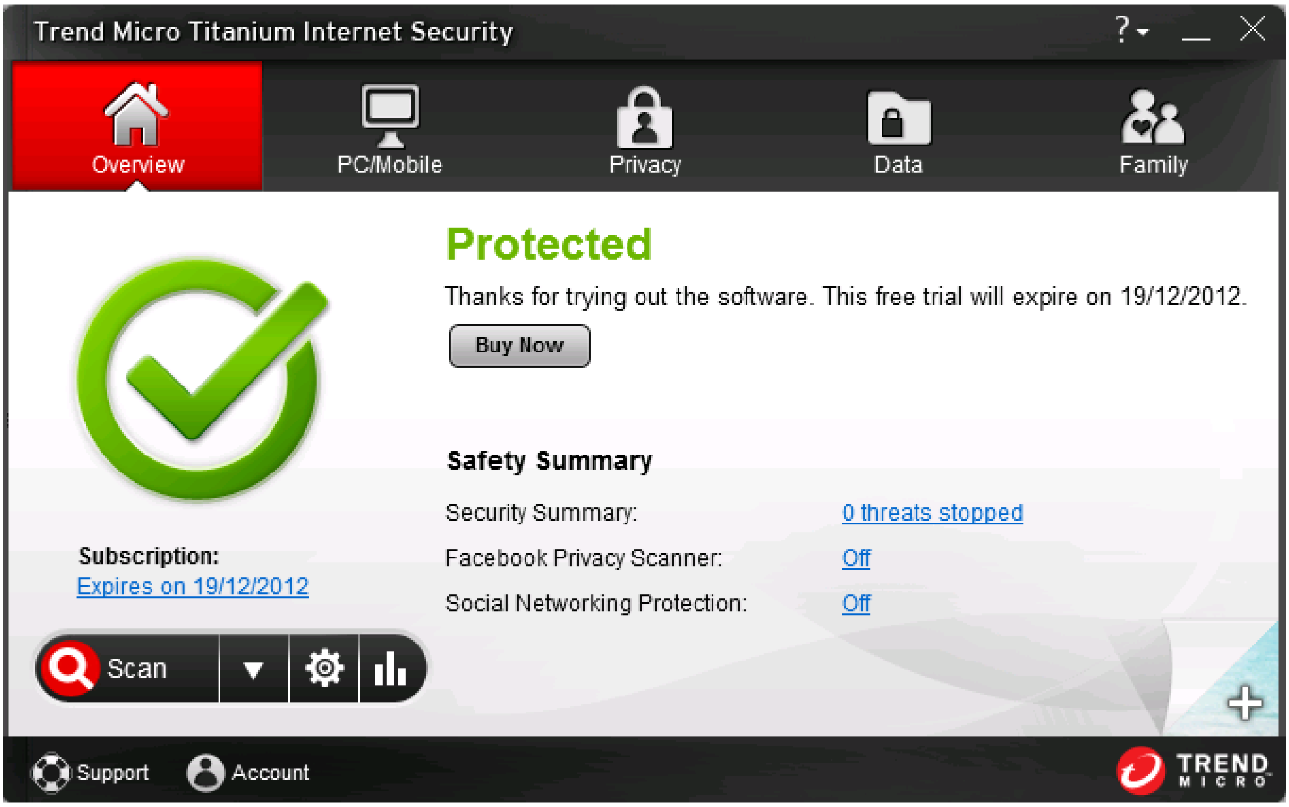
Sophos' website has an extensive knowledgebase feature. A brief test of this suggested that it is so extensive that it can be difficult to find the right answer to a query amongst the many pages of possible articles.

There is a comprehensive manual available for Sophos Endpoint Security. It is 114 pages long, and provides detailed instructions for all the configurable components of the program, as well as a troubleshooting guide and glossary of relevant technical terms. It is clearly written and laid out. There is a simple table of contents with links to the pages mentioned, and the document has been well bookmarked, making it easy to access a particular section from the bookmarks pane of Adobe Reader. Unfortunately there are no screenshots, which we feel is an omission.

Verdict

We found the interface of Sophos Endpoint Protection to be entirely suitable for a managed business product. It is possible for standard users to run scans and update the signatures, but not disable any important components. Default actions and alerts on malware discovery are largely appropriate, with the one exception of malware detected by real-time protection not being removed until the computer is rebooted. The local help function is clear and simple, and is supplemented by a comprehensive manual.

Trend Micro Titanium Internet Security 2013



Protected

Thanks for trying out the software. This free trial will expire on 19/12/2012.

Buy Now

Safety Summary

Security Summary: 0 threats stopped

Facebook Privacy Scanner: Off

Social Networking Protection: Off

Subscription:
Expires on 19/12/2012

Components

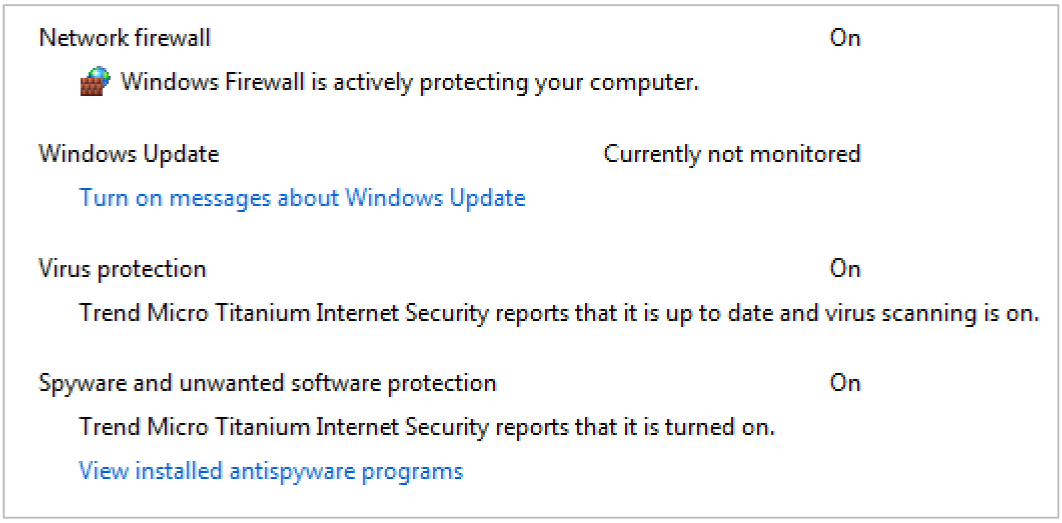
Trend Micro Titanium Internet Security 2013 consists of an antimalware component with email scanning, plus antispam and parental controls. It does not include its own firewall, relying instead on Windows Firewall. However, it does include what it calls a Firewall Booster, which claims to "enhance the protection given by the Windows Firewall and detect botnet programs". We have not included any firewall tests in this review, as we would expect results to be identical to those of Windows Firewall.

Installation

We installed the trial version of Titanium Internet Security, which is supplied as a 6 MB downloader. This saves a 96 MB full installer file in the Windows All Users Desktop folder. Installation requires accepting a licence agreement, and provides options for using the trial version or entering a licence key, changing the installation folder, choosing a language (various European and Asian languages are available), and opting in or out of malware information sharing.

There is no choice of components. A reboot was not required.

Titanium Internet Security registers itself in Windows Action Center as an antivirus and antispyware program. Windows Defender is disabled:



Network firewall On

Windows Firewall is actively protecting your computer.

Windows Update Currently not monitored

Turn on messages about Windows Update

Virus protection On

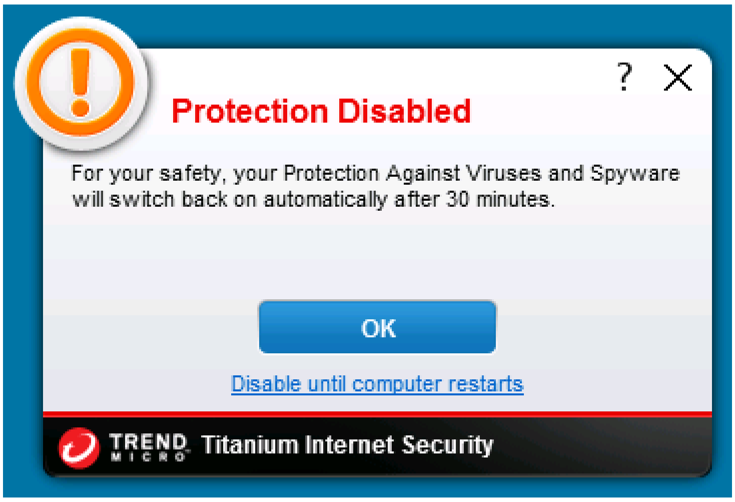
Trend Micro Titanium Internet Security reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On

Trend Micro Titanium Internet Security reports that it is turned on.

View installed antispyware programs

If the real-time protection is disabled, Action Center displays its standard alert. Additionally, Trend Micro displays its own, much more visible warning message, which has to be clicked before it will disappear:



Protection Disabled

For your safety, your Protection Against Viruses and Spyware will switch back on automatically after 30 minutes.

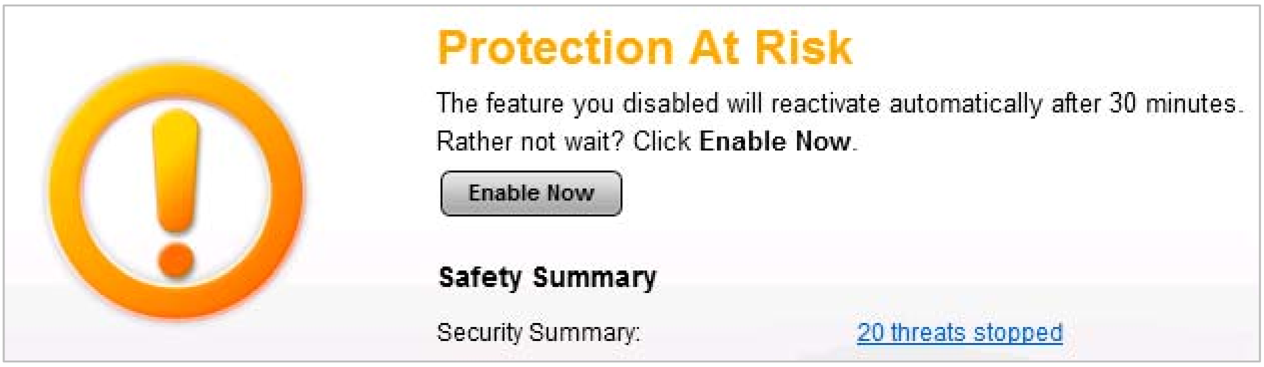
?
X
OK
Disable until computer restarts
TREND MICRO Titanium Internet Security

We consider this a valuable addition to the relatively subtle warning provided by Windows Action Center.

Titanium Internet Security’s uninstaller program has no options other than complete removal.

Program interface

The main program window of Titanium Internet Security consists of a large horizontal status strip, with menu/icon strips at the top and bottom. Security status is shown by a green tick and the word "Protected" if all is well, or a yellow exclamation mark and the wording "Protection At Risk" if an important component is disabled:



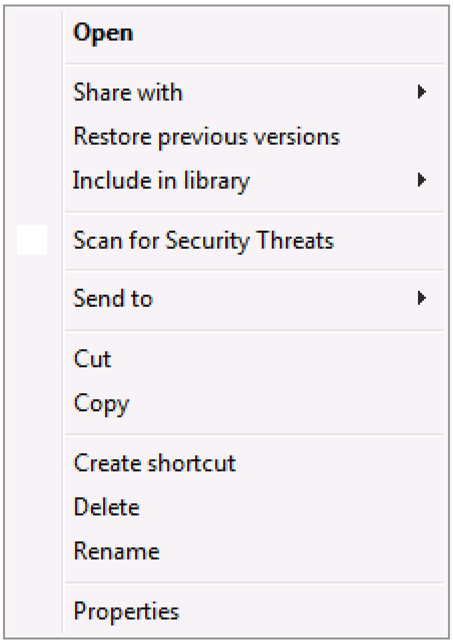
Protection At Risk

The feature you disabled will reactivate automatically after 30 minutes. Rather not wait? Click **Enable Now**.

Safety Summary

Security Summary: 20 threats stopped

A button marked "Enable Now" appears, which will reactivate the component concerned. As Titanium Internet Security 2013 uses cloud-based signatures, there is no update button. There is a prominent Scan button in the bottom left-hand corner of the main panel, which runs a standard scan; a drop-down menu to its left provides the choice of Quick, Full or Custom scans. Trend Micro adds an anonymous "Scan for Security Threats" entry to Windows Explorer's context menu:



Subscription information is clearly displayed in the main panel, and the Support button in the bottom left-hand corner of the window links to the suite's technical support page on the Trend Micro website. The "?" button in the top right-hand corner of the window provides a link to another page of the website, entitled Online Help.

Default configuration

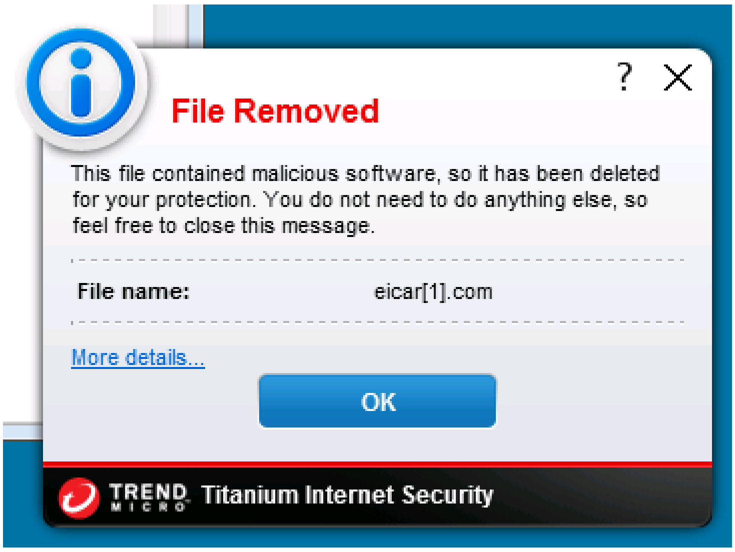
Non-administrator access

When we logged on to our test PC with a non-administrator account, we were able to switch off the real-time protection without any sort of challenge, which we feel is not ideal for a family PC. We note that the settings can be password protected, but there was no prompt from the setup wizard to configure this.

Scanning and malware discovery

A quick scan is scheduled by default every week. This can easily be changed under the settings of Virus & Spyware Controls. We could not find a means of running a boot-time scan, but there are three options for balancing speed of computer startup with degree of protection; the Extra Security option will load the protection components as soon as possible in the boot process.

When we attempted to download the EICAR test file, Titanium Internet Security blocked the download and displayed the following message, which makes very clear that the file has been removed and no further action is necessary:



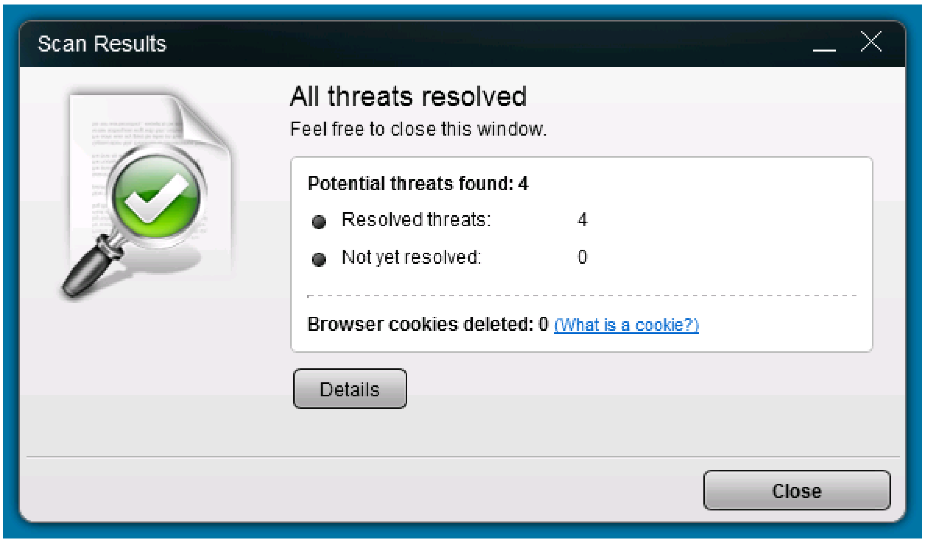
File Removed

This file contained malicious software, so it has been deleted for your protection. You do not need to do anything else, so feel free to close this message.

File name: eicar[1].com

Clicking on More Details shows the log entry with the file name and location, threat name, date and time, and action taken (removed). A similar action was taken when malware was discovered locally by real-time protection.

When we ran a custom or context-menu scan, Trend Micro displayed the following message box; again it is clear that no further action is needed, but details can be seen by clicking on the link:



Scan Results

All threats resolved

Feel free to close this window.

Potential threats found: 4

- Resolved threats: 4
- Not yet resolved: 0

Browser cookies deleted: 0 (What is a cookie?)

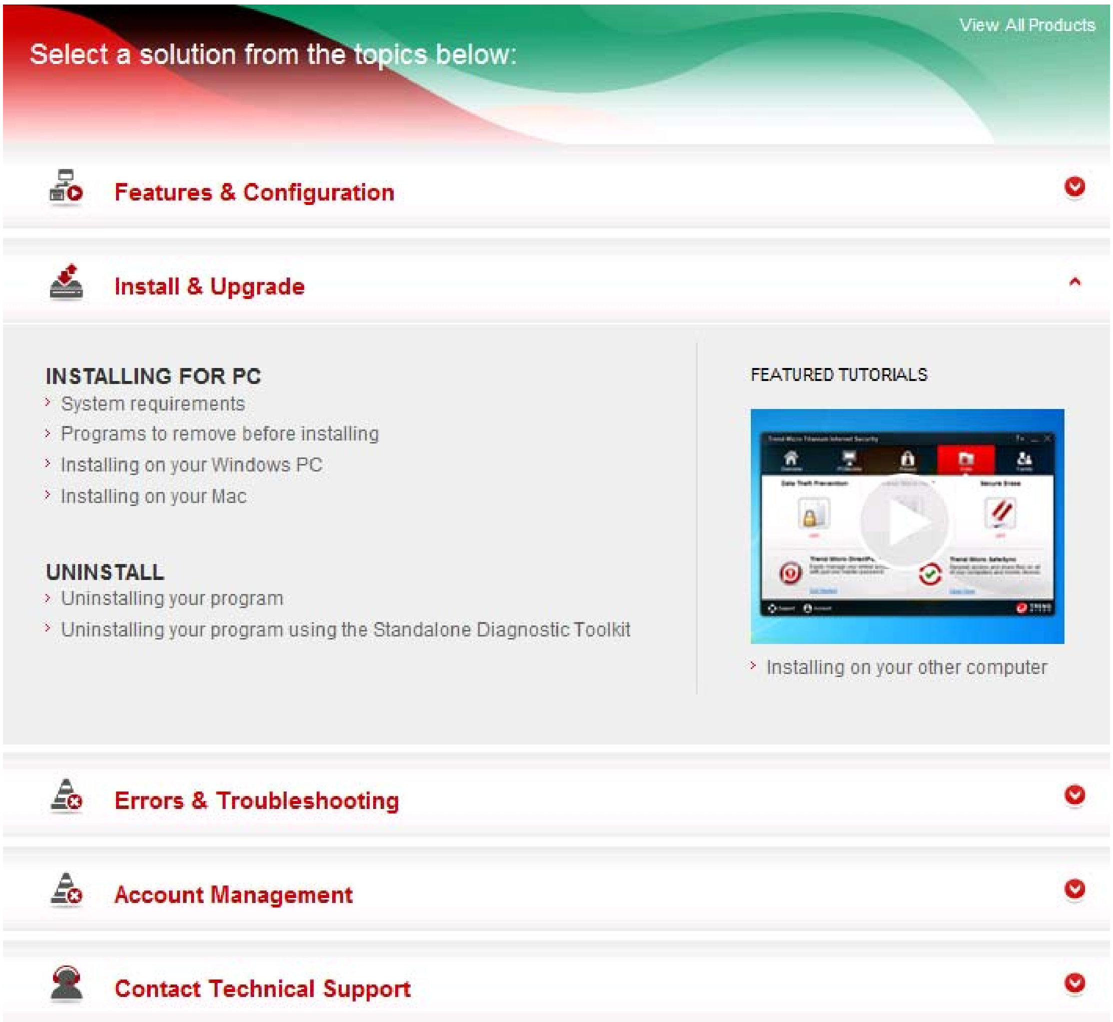
Safe Mode

When we started our test PC in Safe Mode with Networking, we were unable to open the Trend Micro Internet Security Interface; all that appeared was a message box telling us to “Switch out of Safe Mode”. The scan entry on Windows Explorer’s context menu had gone, so we were unable to run any sort of scan.

Help and documentation

The Online Help, accessible from the “?” symbol on the main program window, provides similar functionality to a Windows Help file. We searched for instructions on scheduling a scan; only one result was returned, but this was exactly what we wanted, providing clear, concise instructions for the task. Our second search, for scan exceptions, was also successful, although using the plural “exceptions” as a search term failed to find any results, whereas the singular “exception” found what we were looking for.

The Technical Support pages, found by clicking on Support in the bottom right-hand corner of the main window, could be likened to a manual, with specific tasks listed in different sections. We note that some video tutorials are also available:



View All Products

Select a solution from the topics below:

Features & Configuration

Install & Upgrade

INSTALLING FOR PC
- System requirements
- Programs to remove before installing
- Installing on your Windows PC
- Installing on your Mac

UNINSTALL
- Uninstalling your program
- Uninstalling your program using the Standalone Diagnostic Toolkit

FEATURED TUTORIALS
- Installing on your other computer

Errors & Troubleshooting

Account Management

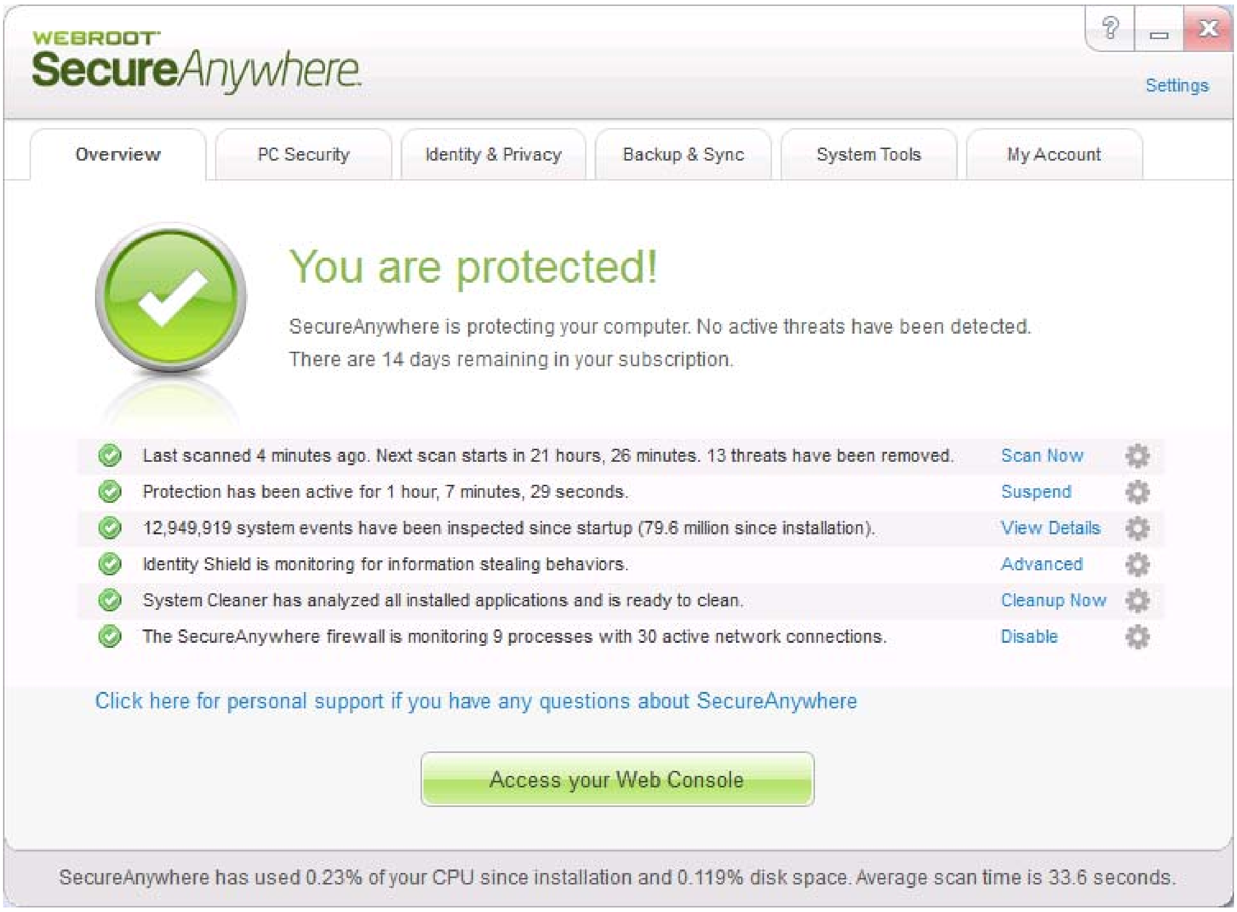
Contact Technical Support

There is a comprehensive 134-page manual available on the website. This covers all aspects of installing, configuring and using the suite, and even has separate installation instructions for Windows 8, in addition to those for Windows 7. The manual is clearly written, well structured, and abundantly illustrated with appropriate screenshots. Unfortunately, there are no bookmarks, but the contents page has hyperlinks to the pages/sections listed, which helps to find the required page quickly and easily.

Verdict

We found Trend Micro Titanium Internet Security 2013 to be very easy to install and use. The interface makes all important information and features easily accessible, and we consider the warning messages to be excellent. The help functions also appear to be good. Two suggestions for improvement would be to prevent by default any unauthorised users from disabling the protection, and to enable scanning in Safe Mode.

Webroot SecureAnywhere Complete 8.0



You are protected!

SecureAnywhere is protecting your computer. No active threats have been detected.
There are 14 days remaining in your subscription.

Last scanned 4 minutes ago. Next scan starts in 21 hours, 26 minutes. 13 threats have been removed. Scan Now
Protection has been active for 1 hour, 7 minutes, 29 seconds. Suspend
12,949,919 system events have been inspected since startup (79.6 million since installation). View Details
Identity Shield is monitoring for information stealing behaviors. Advanced
System Cleaner has analyzed all installed applications and is ready to clean. Cleanup Now
The SecureAnywhere firewall is monitoring 9 processes with 30 active network connections. Disable

Click here for personal support if you have any questions about SecureAnywhere

Access your Web Console

SecureAnywhere has used 0.23% of your CPU since installation and 0.119% disk space. Average scan time is 33.6 seconds.

Components

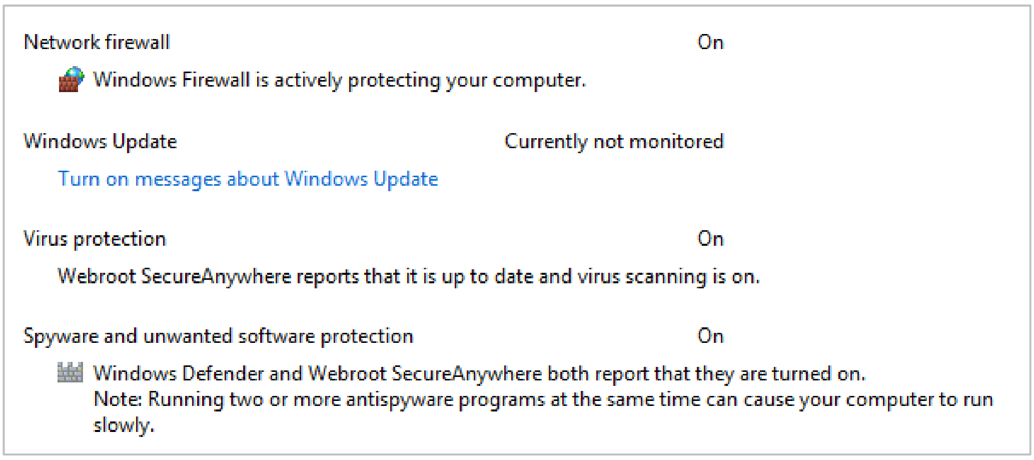
Listing the components included in Webroot SecureAnywhere is not as straightforward as with some other suites, because its functionality does not always fit perfectly into standard categories. We feel that a simple and reasonably accurate description of the program would be "An antivirus and antispyware program with application control, a backup function and shredder". The suite provides the standard functions of an antivirus program, although we understand that there is no email scanner as such; email attachments are only scanned on execution. Neither antispam nor parental controls are included, but there is a shredder (secure deletion function) and an online backup feature that additionally allows data to be synchronised across different devices.

Webroot's website states that SecureAnywhere Complete includes a "two-way firewall". The program interface also includes configuration options for the firewall, including a means of disabling it. However, we have noted below that after installing the Webroot Suite, Windows Action Center shows that Windows Firewall is still running, and does not list any other installed firewall programs. We understand from Webroot that SecureAnywhere uses Windows Firewall for protection against incoming attacks, but adds its own mechanism for monitoring outgoing processes as well. We sympathise with any users who find this confusing, and suggest that Webroot might make things clearer by giving their own component a different name, such as "Application Control".

Installation

We installed Webroot SecureAnywhere from the 712 KB downloader file provided for trial use. The first step of the setup wizard is to enter the licence key. There is an options button, which allows the installation folder to be changed, and offers a modest selection of European and Asian languages. Clicking "Agree and Install" implies acceptance of the licence agreement. There are no other options, and setup completes very quickly. A reboot was not required.

Webroot SecureAnywhere registers with Windows Action Center as an antivirus and antispyware program. It does not register a separate firewall (as noted in the Components section above), and Windows Firewall is not disabled. Windows Defender also remains active:



Network firewall On
Windows Firewall is actively protecting your computer.

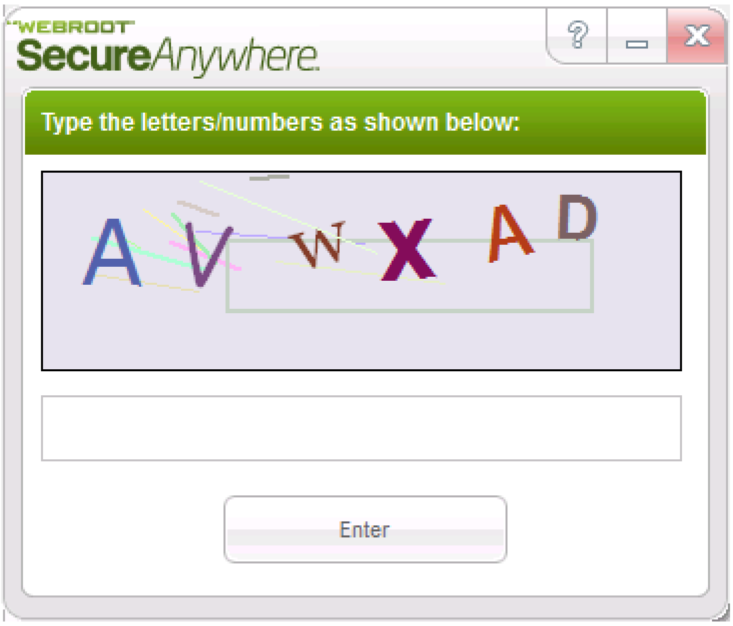
Windows Update Currently not monitored
Turn on messages about Windows Update

Virus protection On
Webroot SecureAnywhere reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection On
Windows Defender and Webroot SecureAnywhere both report that they are turned on.
Note: Running two or more antispyware programs at the same time can cause your computer to run slowly.

The interaction between Webroot SecureAnywhere and Windows Action Center is rather complicated compared to most other security programs. We will describe the various scenarios and let readers decide for themselves whether they consider Webroot's reactions to be appropriate.

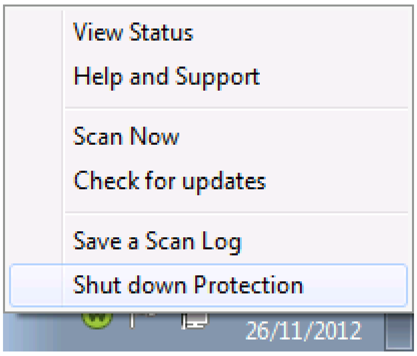
Firstly, we note that if the user attempts to disable any of the protection components using any method, a CAPTCHA dialog is displayed:



Type the letters/numbers as shown below:

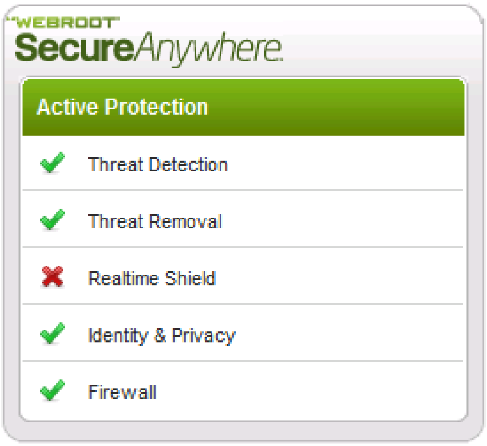
Unless the correct letters are entered, the component(s) concerned will remain active. We regard this as an excellent feature, which would help to prevent malicious programs disabling protection without the user's knowledge.

It is possible to disable all the suite's protection features at once, by right-clicking Webroot's System Tray icon and clicking Shut Down Protection:



When this action is taken, Windows Action Center issues its normal alert, and the Security section show that Webroot's antivirus and antispyware protection are turned off. We note that in this case, the Webroot icon disappears from the system tray. The program can be restarted by (double) clicking any program link on the Windows Desktop, Start Menu or Taskbar. Full protection is then instantly resumed without any further action from the user, and the Action Center warnings are switched off.

If individual protection components such as real-time protection are individually disabled from the program's main window, Windows Action Center does not issue any sort of warning, and continues to show SecureAnywhere's antivirus and antispyware components as functioning normally. However, Webroot displays its own alert in the bottom right-hand corner of the screen:

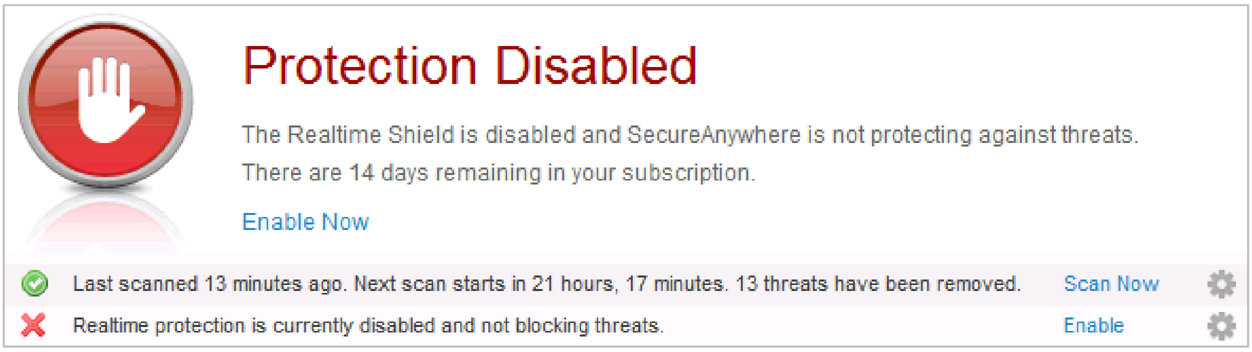


We note that this is only a message box and cannot be used to reactivate the protection; this must be done from the main window. Although the message fades after a few seconds, if the user signs out of Windows and then in again while the protection is still disabled, Webroot's alert will be shown again at logon. When real-time protection is reactivated from the main program window, a short scan is run automatically immediately afterwards, which strikes us a sensible precaution.

SecureAnywhere's uninstaller has no options other than complete removal.

Program interface

The Overview (home) page of SecureAnywhere's main program window features a prominent status display at the top, consisting of a tick (checkmark) in a green circle, and the text "You are protected!" if all is well. Six smaller symbols and lines of text in the main part of the window show the status of individual components, along with links to configure/start each item. If real-time protection is disabled, the main status display text changes to "Protection Disabled", with details in smaller text below. Additionally, the main status icon changes to a hand in a red circle, and the relevant component's own status line changes too:



Protection Disabled

The Realtime Shield is disabled and SecureAnywhere is not protecting against threats.

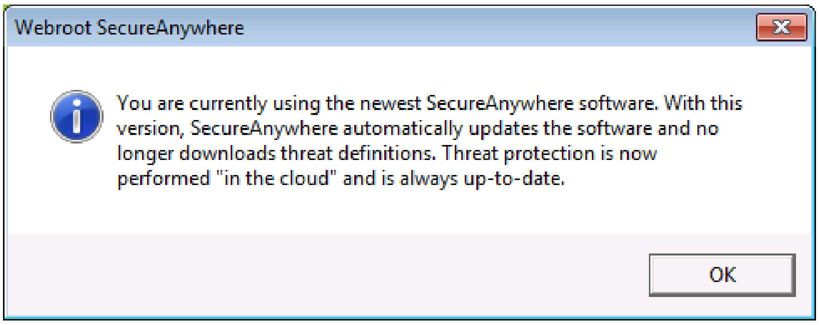
There are 14 days remaining in your subscription.

✓ Last scanned 13 minutes ago. Next scan starts in 21 hours, 17 minutes. 13 threats have been removed.

✗ Realtime protection is currently disabled and not blocking threats.

The main status display shows a link to reactivate the protection, as does the component's own entry.

There is no update button in the main program window, but the context menu displayed when the Webroot System Tray icon is right clicked (please see screenshot of this in the previous section) includes the entry "Check for updates". However, clicking on this produces the following message box, which explains that the current version of the program does not download malware signatures:



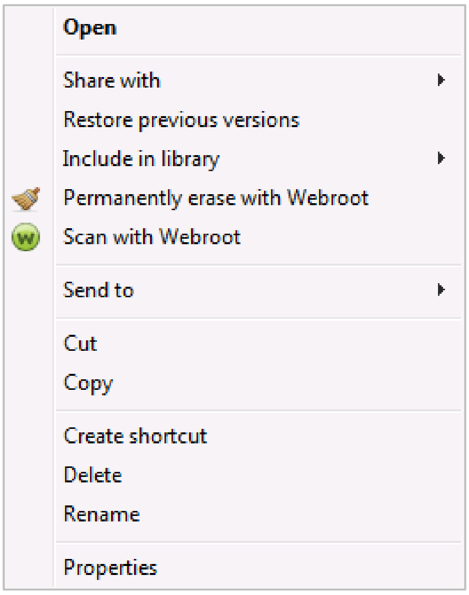
Webroot SecureAnywhere

You are currently using the newest SecureAnywhere software. With this version, SecureAnywhere automatically updates the software and no longer downloads threat definitions. Threat protection is now performed "in the cloud" and is always up-to-date.

Subscription information is shown in the main status display at the top of the window. A quick scan can be started from the Scan Now link on the home page. A custom scan can be run by clicking the PC Security tab at the top of the window, and clicking the Custom Scan link on this page.

Help functions are accessed by clicking the "Click here for personal support if you have any questions about SecureAnywhere" link at the bottom of the home page.

SecureAnywhere's shredder and malware scanning functions are integrated into Windows Explorer's context menu:



Default configuration

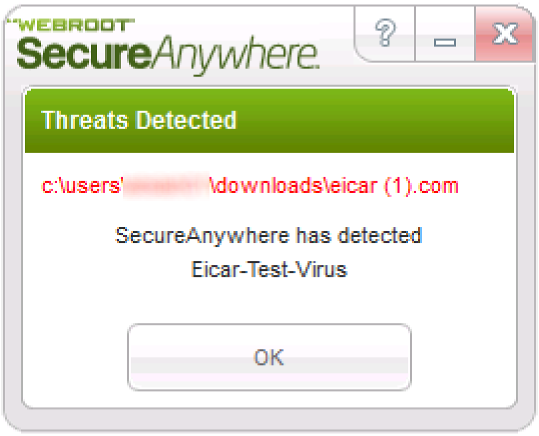
Non-administrator access

When we logged on to our test PC with a non-administrator account, we were able to deactivate individual protection components, and shut down the program completely, without having to provide administrator credentials (although we still had to fill in the CAPTCHA prompt). We do not consider this to be ideal, especially if the suite is installed on a computer intended for family use. It is possible to change the configuration in the Advanced Settings, so that non-administrator accounts cannot disable protection, although there is no mention of this in the setup wizard.

Scanning and malware discovery

A scheduled scan is configured by default in SecureAnywhere. It can easily be changed by clicking the PC Security tab and then Change Scan Schedule. The same page can be used to run a boot-time scan if the computer is off at the scheduled time.

When we attempted to download the EICAR test file, we found that the download completed and was visible in the Downloads folder for a few seconds, after which Webroot deleted it, and displayed the following alert:



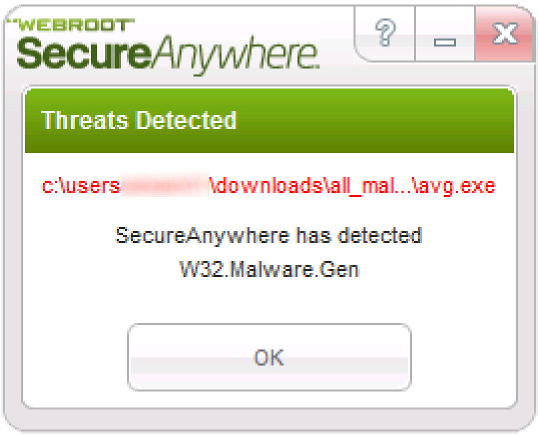
Threats Detected

c:\users\[redacted]\downloads\eicar (1).com

SecureAnywhere has detected
Eicar-Test-Virus

We note that the EICAR file reached the Windows Downloads folder, and was detected by Webroot SecureAnywhere there and quarantined. Although the initial alert only states that a threat has been detected (rather than blocked or removed), a subsequent quick scan is performed, which displays a report on the action taken.

When Webroot's real-time protection discovered malware locally on our PC, it displayed a similar message box:

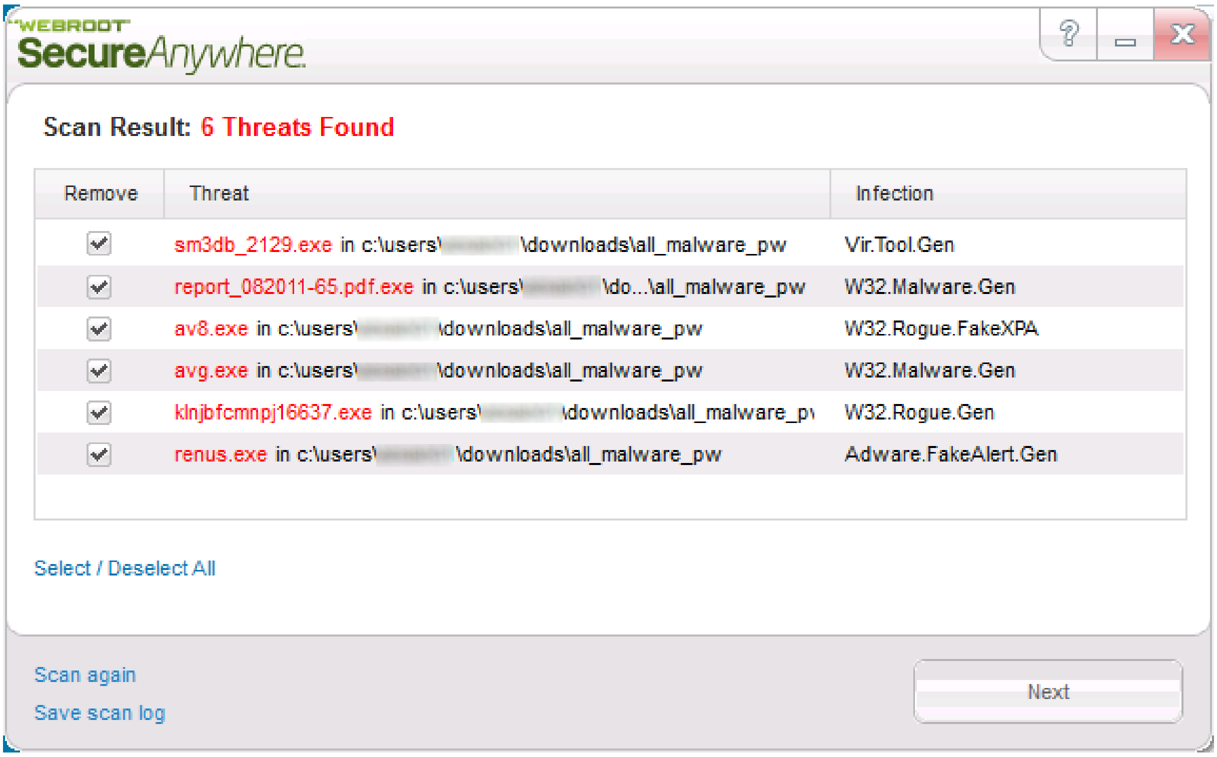


Threats Detected

c:\users[redacted]\downloads\all_mal...\avg.exe

SecureAnywhere has detected
W32.Malware.Gen

SecureAnywhere then ran a quick scan of the folder, with identical results to the custom scan described below. Running a custom or context-menu scan presented us with a list of malware items found; clicking Next quarantined them:



Scan Result: 6 Threats Found

Remove	Threat	Infection
☑	sm3db_2129.exe in c:\users\[redacted]\downloads\all_malware_pw	Vir.Tool.Gen
☑	report_082011-65.pdf.exe in c:\users\[redacted]\do...\all_malware_pw	W32.Malware.Gen
☑	av8.exe in c:\users\[redacted]\downloads\all_malware_pw	W32.Rogue.FakeXPA
☑	avg.exe in c:\users\[redacted]\downloads\all_malware_pw	W32.Malware.Gen
☑	klnjbfcmnpj16637.exe in c:\users\[redacted]\downloads\all_malware_pw	W32.Rogue.Gen
☑	renus.exe in c:\users\[redacted]\downloads\all_malware_pw	Adware.FakeAlert.Gen

Inbound firewall settings

As we understand that SecureAnywhere relies entirely on Windows Firewall for protection against incoming attacks, we ran a very simple test to verify this. In the Network and Sharing Center of our test PC, we set the network type to Public. We then ascertained that ping, file-sharing and Remote Desktop access were completely blocked. After this, we disabled Webroot's firewall component and repeated the tests; as expected, this made no difference at all, as all forms of access were still blocked.

Outbound firewall/application control

When we ran our firewall testing program, we found that it was able to complete its task without any form of query from Webroot, which we consider ideal. Webroot inform us that each application is monitored and its behaviour assessed before allowing Internet access. Advanced users can block individual applications in the firewall settings if desired.

Scanning without cloud access

As Webroot SecureAnywhere uses its cloud service for malware detection, we performed a simple test to get an idea of how it behaves when offline, i.e. when the computer does not have an Internet connection, and so the program cannot access its database on the server. This simulates a situation where a laptop user connects a USB flash drive containing malware to their computer when offline.

The test should not be seen as an effective malware detection test, as it used only 6 Trojans and the EICAR test file (although the results are supported by the vastly more extensive lab tests carried out by AV-Comparatives). The purpose is to see whether the program warns that its detection capabilities are reduced when there is no access to the cloud.

The test was done on a newly installed system which had not been used for malware testing previously, to exclude the possibility that Webroot SecureAnywhere had locally cached signatures of malware it had already detected with a cloud connection. As with our other scanning tests, Windows Defender was disabled.

To run the test, we disabled the network adapter on our test PC, restarted the computer, and checked that there was no network/Internet access. We next opened SecureAnywhere, and checked whether the program displayed any warning to the effect that it was offline, which it did not. We then unzipped and scanned our folder of malware, to see if the program was able to identify any of the items without cloud access. We found that SecureAnywhere was able to identify the EICAR test file, but none of the other items, even though it had been able to detect all of them when an Internet connection was available. Again, there was no warning that the PC was offline. We conclude that the program may rely substantially on cloud access to detect malware, and suggest that it should warn users when it is not able to connect to its servers. When the test PC was offline, we noted that the Status page claimed that SecureAnywhere was monitoring a number of “active network connections”, which we found misleading.

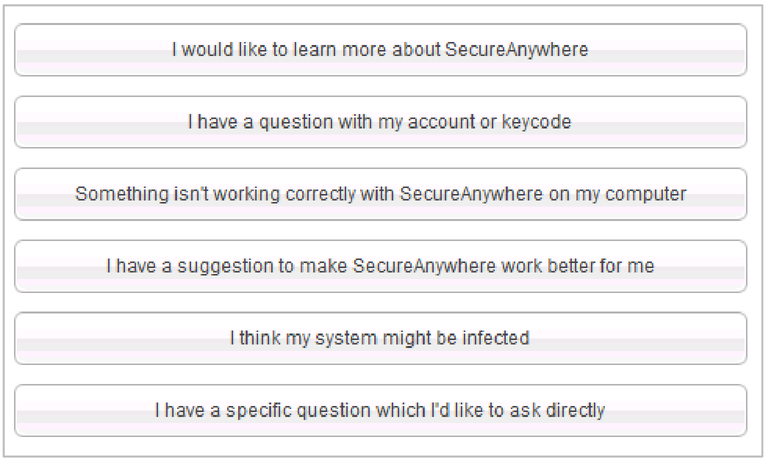
Webroot tell us that if any malware is executed when the computer is offline, SecureAnywhere will clean the system up when network access is restored, and that any files modified by the malware will be replaced by copies of the pre-infection state.

Safe Mode

When we started our test PC in Safe Mode with Networking, we found that Webroot SecureAnywhere was fully functional and behaved exactly as it would in standard mode. Real-time protection was running and quarantined malware on detection, and scans ran entirely normally. We find this commendable.

Help and documentation

Clicking on the long support link at the bottom of SecureAnywhere's window opens the following dialog box:



I would like to learn more about SecureAnywhere

I have a question with my account or keycode

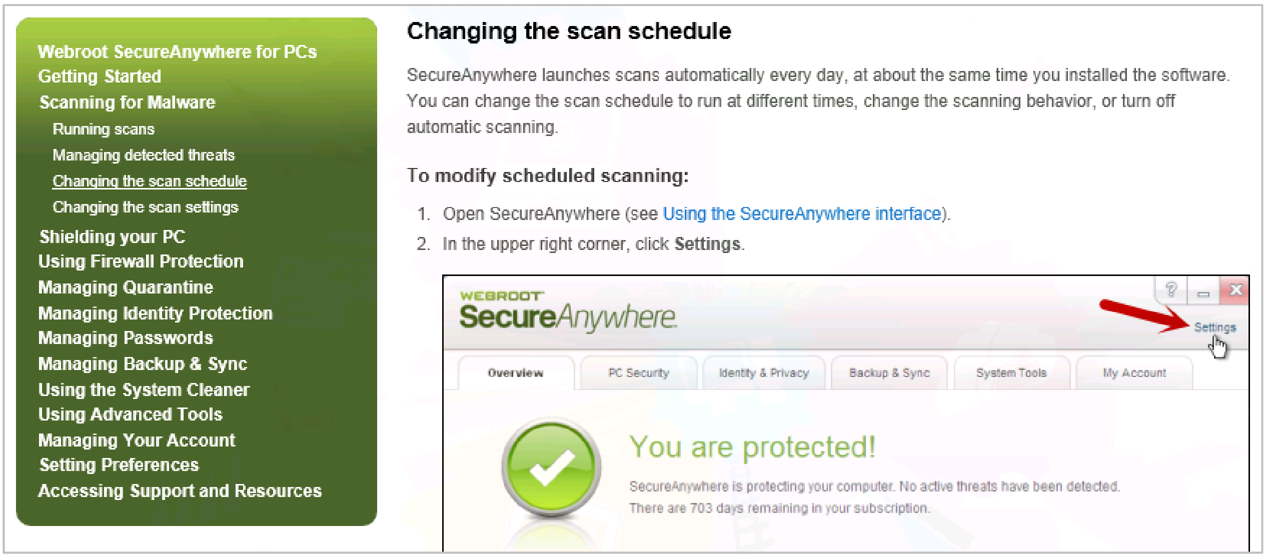
Something isn't working correctly with SecureAnywhere on my computer

I have a suggestion to make SecureAnywhere work better for me

I think my system might be infected

I have a specific question which I'd like to ask directly

All the buttons are links to pages on the Webroot website. The top one of these, "I would like to learn more about SecureAnywhere", leads to what could be described as an online manual. This page has a list of topics in a box on the left-hand side of the page, each of which expands when clicked to reveal sub-topics. The details of a selected sub-topic are shown on the right. We found the instructions to be clear and simple, and well illustrated with screenshots:



Webroot SecureAnywhere for PCs
Getting Started
Scanning for Malware
- Running scans
- Managing detected threats
- Changing the scan schedule
- Changing the scan settings

Shielding your PC
Using Firewall Protection
Managing Quarantine
Managing Identity Protection
Managing Passwords
Managing Backup & Sync
Using the System Cleaner
Using Advanced Tools
Managing Your Account
Setting Preferences
Accessing Support and Resources

Changing the scan schedule

SecureAnywhere launches scans automatically every day, at about the same time you installed the software. You can change the scan schedule to run at different times, change the scanning behavior, or turn off automatic scanning.

To modify scheduled scanning:

1. Open SecureAnywhere (see Using the SecureAnywhere interface).
2. In the upper right corner, click **Settings**.

WEBROOT
SecureAnywhere
Settings
Overview
PC Security
Identity & Privacy
Backup & Sync
System Tools
My Account
You are protected!
SecureAnywhere is protecting your computer. No active threats have been detected.
There are 703 days remaining in your subscription.

As seen in the screenshot above, it is easy to find instructions on scheduling a scan. We were unable to find any instructions relating to scan exclusions, however.

There is also a downloadable manual for Webroot SecureAnywhere. It is very comprehensive, at 199 pages, and has been abundantly illustrated with appropriate screenshots. It covers installation, configuration and use of the suite. There is a comprehensive table of contents, with each item being hyperlinked to the relevant page. Suitable bookmarks also make it easy to navigate the document from Adobe Reader's Bookmarks Pane. Instructions are clear and simple.

Verdict

The installation of Webroot SecureAnywhere is very quick and straightforward. We found the program's main window to be quite simple and effective, enabling the user to find important functions and information without any difficulty. Other aspects of the program might prove a little confusing to some users, however. These include the use of the term "firewall" to describe a feature that we would prefer to describe as "application control", and the claim in the status section that the program is monitoring a number of active network connections when the network adapter is disabled and there is no form of network connectivity at all. We were impressed with the use of a CAPTCHA device to protect critical settings from malicious programs, and the program's full functionality in Safe Mode with Networking. Our main suggestions for improvement would be showing a warning when cloud signatures cannot be reached, and preventing non-administrator accounts from disabling protection.

The AV-Comparatives team and Webroot have together decided not to include the new SecureAnywhere product line in the 2013 public main-test series. AV-Comparatives recognizes that Webroot's approach to protecting the user (preventing unauthorized data transmission, combined with protocolling changes and reversing them where possible) would require a different test procedure which is not applied by any testing lab so far. Unfortunately, such a test could in some cases take several days for each single test case to be performed, making it almost impossible to perform a statistically valid test with results comparable with the ones of other security solutions. AV-Comparatives will work with Webroot to investigate the feasibility of developing a test that will assess SecureAnywhere's protective abilities and allow for comparison with other products.

Copyright and Disclaimer

AV-Comparatives e.V. and its testers cannot be held liable for any damage or loss which might occur as a 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 liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives e.V. 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. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

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

Translation: David Lahee

AV-Comparatives e.V. (January 2013)