

Q&A

What's new

- Improved scanning technology, better user experience, browsing protection and Windows 7 support.
- All new and task-focused user interface offers enhanced usability.
- Core technology improvements for malware and spyware detection and removal.
- Browser protection to prevent infections from malicious websites.
- Parental Control, Spam Control and Application Control use in-the-cloud technology to guide the user and make automatic decisions more effectively.
- Fully automatic malware removal, improved performance and optimized default settings.

Q: How do I install F-Secure Internet Security 2010?

A: Download the solution from <ftp://is2010:FkLerT47Hk@ftp.customer.f-secure.com/> or – after September 3, 2009 – from <http://download.f-secure.com/estore/fs2010.exe> and use the subscription key provided to you.

Q: How big is the installation package?

A: The installation package for F-Secure Internet Security 2010 is 70MB and the initial download during installation is 30 MB.

Q: What has happened to the user interface? It has changed from the 2009 version.

A: F-Secure's User Experience team did extensive research and testing among users to discover their most common tasks and needs for a security service. The research showed that users open the user interface only when they need to perform a specific task. By changing the user interface into one that is task-focused, users can quickly get to what they want. The "Update Now" and "Scan" buttons are now on the front page and the settings are grouped logically.

Q: What is the F-Secure Real-Time Protection Network (RTPN)?

A: The F-Secure Real-time Protection Network, also known as "in-the-cloud" protection, is a web service hosted in large datacenters around the world containing information on good and malicious files and websites. It is an important part of the browser protection component and is also used by the DeepGuard functionality. DeepGuard is a proactive protection technology that employs behavioral analysis and the Real-Time Protection Network to provide protection against threats.

Q: Can I turn off the Real-Time Protection Network?

A: Yes you can. However, deactivation of real-time protection disables some whitelisting and deactivation of DeepGuard disables most of the heuristics and process protection.

Q: What is DeepGuard Advanced Process Monitoring?

A: Advanced Process Monitoring is a functionality of DeepGuard. It protects the browser from hijacking and remote control attempts, prevents the installation of malicious drivers and protects F-Secure's own processes.

Q: Why do some games report being illegal versions when DeepGuard Advanced Process Monitoring is enabled?

A: DeepGuard Advanced Process Monitoring works by modifying the memory of every running process to enable monitoring of suspicious events. This is known to cause some problems with copy protection and anti-cheating software, especially used in games. The games in question may refuse to start because integrity checks or checks for genuine software fail, or they might crash during copy protection checks and players could be kicked out of online games because they are falsely detected as “cheaters”. These issues are constantly being monitored and fixed by our Labs as new games and protection mechanisms are released to the market.

Q: What should I do if I suspect DeepGuard Advanced Process Monitoring is preventing a legitimate program from running?

A: You can always disable DeepGuard Advanced Process Monitoring without compromising your system as long as you carefully consider where you surf and which files you download or open on your computer. If the problems only occur with DeepGuard APM enabled, we would appreciate feedback about the affected application so that we can take actions accordingly.

Q: What are the color codes in my browser?

A: Color-coded website safety ratings (Safe - Green, Suspicious - Yellow, Malicious – Red, Not rated – Gray) are shown in the browser toolbar whenever a website is visited. Safety ratings for links in search results and web-based e-mails are shown before a user has an opportunity to click on a link. Based on these ratings, the user can make an informed decision whether to click on the link.

Q: Why are some websites being blocked by my browser?

A: The RTPN actively blocks access to malicious websites that are a clear threat to the computer or personal information due to active malicious content like exploits or phishing. Despite blocking a page, the user can open the site by selecting the link on the blocking page. Clicking “This site is: SAFE” and then “Security summary for this website” will show F-Secure’s opinion.

F-Secure Browsing Protection also includes a brand new technology called F-Secure Exploit Shield which provides active protection against previously unknown websites containing exploits. Exploit Shield has specifically been developed to protect against these “drive-by download” infection attempts. It can also be used by F-Secure to provide protection against specific browser vulnerabilities before the software provider publishes a patch. This is done using “shields” that block attempts to use the vulnerable part of the browser.

Q: How can I report unrated URLs?

A: Unrated URLs that have gray rating can be reported to F-Secure for testing or already rated URLs can be sent for re-rating. The button “Notify us” sends the URL to F-Secure’s RTPN to be checked.

Q: If I purchase a new PC with Windows 7 OS, will F-Secure Internet Security be compatible? Will the new version discontinue support for any older OS?

A: Yes it will. F-Secure Internet Security 2010 supports the upcoming Microsoft Windows 7 operating system. It also supports the Microsoft Windows XP and Microsoft Windows Vista operating systems. However, we no longer support Microsoft Windows 2000 Professional.

Q: How does the safety rating plug-in work?

A: Whenever it needs to show a safety rating for a URL, the browser plug-in queries the F-Secure Real-time Protection Network to get the rating. The Real-time Protection Network contains ratings for tens of millions of different URLs which are based on URL analysis by various backend systems in F-Secure Labs. Contributions to the network can be turned off in the user interface.

Q: How has the parental control functionality changed from the previous version of F-Secure Internet Security?

A: Parental Control now utilizes RTPN for evaluating sites. It provides more accurate results and faster reaction times for emerging non-appropriate content.

Q: Has spam control changed in some way?

A: Changes have also been made in the core technology of Spam Control and it utilizes RTPN. The anti-spam feature is always optimized for currently active spam e-mails. This may affect detection rates when out-of-date spam sample collections are used.

Q: Why do many leak tools execute and run successfully on a machine that is protected by F-Secure Internet security 2010?

A: In most cases, leak tools send data to the internet to prove that data can “leak” through the firewall. To do this they are using various techniques that are also used by other, legitimate and harmless software.

In F-Secure Internet Security 2010 the Anti-Virus and Firewall components work closely together to prevent malicious actions of programs or code. When an application is executed, its behavior is monitored and an assessment done whether its actions are potentially dangerous.

Leak tools are by definition legitimate applications from well known sources and in many cases even digitally signed. They are not destructive or dangerous in any way. They are therefore detected correctly as harmless and allowed to execute.

Q: Can malware that uses the same technique than a leak tool run undetected?

A: Definitively not. DeepGuard is capable of distinguishing whether a certain technology or technique is used as an attack vector by a malicious application or if it is normal operation of benign software. In other words, just because a certain procedure is also used by malware, not all applications using the same techniques are discredited. Doing so would block a great deal of legitimate software from running or at least increase the noisiness of the software enormously. Instead of looking at a single action, DeepGuard assesses the actual threat the software poses to the user’s safety or privacy.

Q: How can I test how leak tools are detected by F-Secure Internet Security 2010?

A: Some actions performed by leak tests are detected by DeepGuard and are considered potentially dangerous, which leads to a popup asking for permission. To see the dialog for all applications performing actions that trigger DeepGuard’ decision logic (not just the applications DeepGuard considers dangerous), set DeepGuard to ‘Expert Mode’ by choosing the most interactive setting “Always ask me”. Even with the ‘always ask me’ setting enabled, commonly known clean applications are trusted and clearly malicious applications are blocked automatically. The dialog displayed when a new application is launched contains a detailed summary of what actions the software is trying to take.

This way it is also possible to confirm that DeepGuard is carefully monitoring the leak tool and its actions, and has correctly classified it as non-malicious.

Q: Can you give a few examples of software using the same techniques as leak tools?

A: Many leak tools do nothing more than call Internet Explorer and open a certain URL to display a message that the leak has succeeded. The online help of many commercial programs does the same, displaying the help pages requested.

In some cases, leak tools will also transfer data that was generated on the computer to the web pages called to alter the results. This is done to show that the users' valuable data could be funneled to hacking sites. Context-related help sends the user's topic in order to display the answers the user needs to solve the problem at hand.

Q: Why does the first full computer scan take so long?

A: A full computer scan will scan all hard drives for malware, such as spyware, viruses and rootkits. Due to whitelisting the second full computer scan will be significantly faster. This also accounts for differences in numbers of files scanned between scans.

Q: Why does the number of files scanned in subsequent scans vary?

A: The number of files is different because of whitelisting implemented in the F-Secure Internet Security 2010.

Example: If an archive has not changed between scans, then it will not be touched in the second scan. If the archive contains 100 files, then the scanned files number will be 101 higher in the initial scan. A second manual scan will also typically take a matter of minutes.

It should also be noted that scheduled scans may find more viruses than a manual scan. The reason for this is that scheduled scans run as an administrative user, and this user may have access to additional files.

CONTACT INFORMATION

For more information about obtaining software for review purposes or general questions about F-Secure and its products, please e-mail your question to: reviewers@f-secure.com

[F-Secure Press Room](#) provides you illustrations, screenshots and other material.