RELEASE NOTES
F-SECURE INTERNET SECURITY 2013 RELEASE 3

This file contains important information regarding F-Secure Internet Security 2013 release 3. We strongly recommend you read the entire document.

Contents

Release Notes F-Secure Internet Security 2013 release 3 1

New in Internet Security 2013 release 3 2

Installation and System Requirements 2

Operating systems supported 2

System requirements 2

Supported Browsers 3

Details 3

Contact Information and Feedback 3

Known issues 4

Common issues 4

Computer Security 4

Online Safety 4

© 2010 F-SECURE CORPORATION. ALL RIGHTS RESERVED.

New in Internet Security 2013 release 3

- **Banking protection:** Improvements in banking protection when online shopping in less well known online stores. Other minor bug fixes and improvements.
- **Subscription handling improvements:** My Subscription page is rearranged. Install key is now available on the page. Other minor fixes and improvements.
- **Installation improvements:** Installer works better if there are network problems during installation or a proxy is used.
- **Windows Gadget removed:** Microsoft decided to discontinue the use of gadgets and offered the removal of the functionality as a fix for a security vulnerability (MSA 2719662). F-Secure cannot support use of a known to be vulnerable operating system component.
- **Outlook Plugin removed:** Outlook plugin for spam protection is no longer available.

Installation and System Requirements

It is strongly recommended to remove all other anti-virus products before installing F-Secure Internet Security 2013 release 3.

Operating systems supported

- Windows 8 32-bit and 64-bit: all editions.
- Windows 7 32-bit and 64-bit: all editions.
- Windows Vista 32-bit and 64-bit: Service Packs 2 or later.
- Windows XP 32-bit: Home, Professional: Service Pack 3 or later.

System requirements

- Processor: Intel Pentium 4 or equivalent
- Memory: 512 MB or more
- Disk Space: 800 MB free HD space

High speed Internet connection to validate your subscription and receive updates.

The system must fulfill Windows Vista, 7 and 8 minimum requirements as specified by Microsoft

Supported Browsers

Fully supported browsers for Online Safety

- Internet Explorer 7 & 8 (Windows XP), Internet Explorer 8 & 9 (Windows Vista & Windows 7) (32-bit and 64-bit), Internet Explorer 10 (Windows 8)
- Firefox, two latest major versions.
- Chrome, two latest major versions.

Online Safety is implemented in a browser independent way and most browsers will work with Online Safety although they are not officially supported.

Details

- **This release consists of the following applications:** Launch pad 1.77 build 243**,** Computer Security 12.77 build 100**,** Online Safety 2.77 build 1170

- **Localizations are enabled for following 29 languages**: English, Bulgarian, Czech, Danish, Dutch, Estonian, Finnish, French, French (Canadian), German, Greek, Hungarian, Italian, Japanese, Norwegian, Polish, Portuguese, Brazilian Portuguese, Romanian, Russian, Slovenian, Spanish, Spanish (Mexican), Swedish, Turkish, Vietnamese, Traditional Chinese (Hong Kong), Traditional Chinese (Taiwan) and Simplified Chinese.

Contact Information and Feedback

We are looking forward to hearing comments and feedback on the product functionality, usability and performance.

Please report any technical issues through the F-Secure support web site:

http://www.f-secure.com/en/web/home_global/support/get-support-online

If you are reporting a technical problem, please attach F-Secure system summary report to the feedback. To collect the system summary report, you need to have administrator rights.

- In Windows XP, select first Start | All Programs | F-Secure, right-click on Support Tool, select Run as and finally select to run the program as administrator.
- In Windows Vista and 7, select Start | All Programs | F-Secure, right-click on Support Tool and select Run as administrator.
- In Windows 8, right click on the Support Tool tile and select run as administrator.

Known issues

Common issues

When some updates are installed, F-Secure program dialogs are closed automatically
When certain updates are received and installed, it is possible that your open F-Secure program dialogs are closed automatically.

Product got stuck in the upgrading state (system restore problem) (CTS-81468)
Reverting to a Windows restore point which contains previous product version blocks upgrade until new product version is released.

Computer Security

Malware download is still blocked by Web Traffic Scanning, even if Virus and spyware scanning and Firewall are off
Uncheck "Do not allow applications to download harmful files" from Firewall-page to disable web traffic protection.

Unclear scanning counters (LSC-64)
When performing manual scanning, two scanning counters may be shown in some cases, showing incorrect values.

DeepGuard 4 may block some games or applications
If you have problem starting some game or application, enable 'Use the compatibility mode" from DeepGuard page in Computer Security settings and try to start the game or application again. If this does not help, disable also DeepGuard from On/Off -switch from DeepGuard page and try again.

Some applications might be slowed down
You can workaround this by enabling 'Use the compatibility mode" from DeepGuard -page in Computer Security settings.

Some web chat sites may not work with Web Traffic Scanning enabled
Workaround is to disable the Web Traffic Scanning feature.

Online Safety

Web page can be distorted due to page elements' URLs are blocked or have an "unrated" category
This can happen if web page elements (e.g. video, images) is originate from another URL that is "unrated" or have a restricted category or address. You can allow the content by adding the address to the allowed list or reconfigure the category restriction.

Online Safety with "unrated" category enabled may prevent some third party installers from downloading software
If for example the installer uses localhost to read configuration file, Online Safety can

block localhost request because we treated localhost request as unrated. The workaround is to uncheck the "unrated" category.

Applications and games which use HTTP connection will not work properly with Web Filter or Time Limit enabled (PBL-1493)
Application that uses HTTP connection will not work properly when time limit is exceeded. User can reconfigure the web filter unrated category or web filter allowed list or their time limit settings in order for these applications to work normally.

Some functionality is not available when browsing to HTTPS websites (PBL-2195, PBL-2195, CTS-87285)
Search engine rating icon will not be shown if the user searches from a HTTPS website. Also, when browsing to any HTTPS harmful or restricted web site, the web site will be blocked but the blockpage will not be shown.

Blocked elements on small web page frames may not show optimally (CTS-87690)
Websites that uses a small frame which contain a harmful or restricted content will only show partial blockpage.

Notification or settings UI that is launched from Windows 8 Modern UI is not visible.
Any Online Safety notification or settings UI will be shown at Windows 8 desktop mode even though it is launched from Windows 8 Modern UI browser.

Banking protection is not working with Internet Explorer in Windows XP (CTS-90547)
User that are using Internet Explorer with Windows XP are not able to trigger the Banking Protection active.

Chrome live search can start Banking Protection session when it tries to access bank web sites while searching
If Chrome live search is on while you are typing an online bank address, Chrome already opens a connection and this may start Banking Protection session. Workaround is to disable live search.

If bank web page uses unclassified domains to store information, the page is not loaded correctly while in Banking Protection mode.
Turn off Banking Protection from Online Safety user interface and please send us feedback through bankingprotection@f-secure.com.

When using a proxy, proxy IP address needs to be added to allowed websites list
When using a proxy and using Banking Protection you should add proxy IP address to allowed websites list.