# F-Secure PSB Workstation Security 9.30 build 1260
# RELEASE NOTES

## 1. General

This file contains important information regarding F-Secure PSB Workstation Security 9.30. We strongly recommend that you read the entire document before installing the software.

### What's in This File



## 2. Product Contents

This product enables you to install:

- **Virus & spyware protection** with Virus protection, Anti-spyware, E-mail scanning and Web traffic scanning for viruses, Blacklight scanning for hidden malware and the proactive 0-day protection technology DeepGuard™.
- **Network protection** with Firewall, Application control, Intrusion prevention and Dial-up control.
- **E-mail filtering** with protection against spam and phishing.
- **Browsing protection** helps you to protect your personal information which you may have to enter on the Internet when, for example, you subscribe to newsletters, join web communities or do online shopping.
- **Software updater** helps you to keep your system and applications up-to-date by automatically installing patches as they are released by vendors.
- **Automatic updates** keep both the databases and the software up-to-date against the latest threats.

Supported languages are: English, Czech, Danish, Dutch, Estonian, Finnish, French, French (Canadian), German, Greek, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Portuguese (Brazilian), Romanian, Russian, Slovenian, Spanish, Spanish (Latin America), Swedish, Turkish, Traditional Chinese Hong Kong, Traditional Chinese Taiwan, and Simplified Chinese.

## 3. New Features

New features since the release of F-Secure PSB Workstation Security 9.0 include:

 

- **Software updater**

  Software Updater ensures that the operating systems and applications used in your organization are always up-to-date. This lowers the security risks of using vulnerable or unpatched software. It proactively scans the computer for missing security patches and software updates including service packs, and deploys them automatically or on scheduled intervals.

- **DeepGuard 4**

  DeepGuard™ version 4 offers improved malware detection rate. Comparing to the previous version some additional advanced behavioral analysis techniques were added.

- **Windows 8 limited support**

  The product can be installed to Windows 8. However, some incompatible features: Browsing protection, Web traffic scanner - are not installed in Windows 8. Also the product does not support Windows Store applications of Windows 8. The end-point user needs to switch to the traditional Desktop to interact with the product.

- **Korean localization**

  The product is localized to Korean language.

# 4. Fixed issues

**Fixed issues since the release of F-Secure PSB Workstation Security 9.0:**

### DeepGuard does not protect services in Windows 7 [65247]

When stopping a protected service from the command line or from Services, DeepGuard does not prompt about it. However, it still protects services from the most malicious stop attempts. This occurs only in 32-bit operating systems.

### Fetching E-mails from POP3 account using Outlook 2010 hangs [85050]

Fetching e-mails from POP3-Account using OL2010/Win7 hangs at 14 Bytes out of 237KB. Timeout is raised to 5 minutes now.

# 5. Installation and System Requirements

## 5.1. Supported operating systems

- Windows XP 32-bit: Home, Professional and Media Center editions with Service Pack 3.
- Windows Vista 32-bit and 64-bit: all editions, all Service Packs.
- Windows 7 32-bit and 64-bit: all editions and Service Packs.
- Windows 8 32-bit and 64-bit.

 

## 5.2. System requirements

### Microsoft Windows 7, Windows 8, and Vista

- Processor: Intel Pentium 4 2GHz or higher
- Memory: 1GB on 32-bit systems / 2GB on 64-bit systems or more
- Disk space: 900 MB free HD space (600 MB for Anti-virus only)
- Display: 16-bit or more (65000 colors), resolution 1024 x 768
- Internet Connection: An Internet connection is required to validate your subscription, to receive product updates, and to use the cloud-based detection

### Microsoft Windows XP

- Processor: Intel Pentium III 1Gz or higher
- Memory: 512 MB or more
- Operating System: Microsoft Windows XP SP3
- Disk space: 900MB free HD space (600 MB for Anti-virus only)
- Display: 16-bit or more (65000 colors), resolution 800 x 600
- Internet Connection: An Internet connection is required in order to validate your subscription, to receive product updates, and to use the cloud-based detection

# 6. Known issues

## 6.1. Installation and Uninstallation

### Installation to Windows 8 does not install Browsing protection and Web traffic scanner

Due to incompatibility issues, these two features are not installed to Windows 8.

### Reinstallation after using System Restore to remove the product fails [65406]

When the product is installed, a “restore point” is created before the installation. You can use the System Restore feature of Windows to restore the system to the state where it was before installing the product.

However, due to the design of Windows System Restore, the system is not restored to a completely clean state. System Restore is designed to affect executable files (like .exe and .dll) and certain configuration files (like .ini), but not data files (like documents, images and databases, for example). As a result, the product installation folder contains a number of data files, in particular various virus signature files and certain configuration files, after the System Restore operation.

These remaining files cause problems when the product is reinstalled to the system again. Installation is partly successful, but downloaded updates cannot be installed and the product never achieves a completed installation state.

Instead of using System Restore to remove the product, uninstall it using Control Panel’s “Add and Remove Programs” (XP) or “Programs and Features” (Vista). After uninstalling the product and restarting the computer, the product can be installed successfully again.

 

If you have used System Restore to remove the product, delete the folder of the product's binaries (typically "C:\Program Files\F-Secure") including all files and subfolders, before reinstalling the product to make sure the installation can complete.

### Some localizations (e.g. Estonian) can only be installed when the proper system codepage is configured [77201]

When the product installer starts, you can select localization among the languages that can be properly displayed on the system code page. Other languages do not show up in the list. For example, if you work with Estonian language, make sure that your computer's system code page is set to Baltic ANSI 1257. The system code page can be changed in the Regional Settings, "Language for non-Unicode programs". Restart is usually required to take the new setting into use.

### Application control might warn about Ih8run.exe during channel upgrade from earlier versions [61835]

Application control may warn about the F-Secure process "ih8run.exe" during the channel upgrade from an earlier version when the installation dialog shows that updates are being downloaded. It is safe to trust this application.

### Unused databases are still visible for some time after upgrade

During an upgrade, some databases and engines used by the previous version may not be needed anymore. These items are still visible in "Settings – Other settings – Downloads", marked as "Not Installed". This is normal and they are removed automatically after 7 days.

### Inconsistent Post Installation dialog information regarding updates

During the installation of certain updates, such as customizations or hot-fixes, the post installation dialog may show inconsistent information about installed updates. For example, it may change from "Installing update 3/10" to "Installing update 10/10" and then back to "Installing update 4/10". The situation recovers shortly by itself to show the real status.

### Users without administrative rights will not be notified of major product upgrades

Users who do not have permission to install an upgrade do not see that the upgrade is available. The upgrade is listed on the Downloads page in Settings, but the product does not prompt to install it unless you are logged in to a Windows account with permissions to complete the installation.

### Check for updates task might be slow if using Internet browser proxy settings

When Automatic Update Agent is configured to use the browser's HTTP proxy settings and the browser is set to automatically detect proxy settings, the "Check for updates" task may finish slowly as Automatic Update Agent waits for the Internet browser to resolve the proxy settings.

### Quarantine is cleaned on upgrade from the previous version [89426]

If you had quarantined files in the previous version of the product, they are lost after the upgrade to the new version. If you need them, restore them from the quarantine to a folder and include this folder to exclusions from real-time scanning before the upgrade.

 

## 6.2. Firewall, Application Control, Intrusion Prevention and Dial-up Control

### Firewall malfunctions if Vista's Base Filtering Engine service is disabled [53524]

Do not disable the Base Filtering Engine service on Vista platforms. F-Secure Firewall does not work without it.

### PSB TP is not changing firewall profile automatically like Client Security [89396]

If a notebook disconnects from the office LAN and connects to Wi-Fi, the Firewall profile stays unchanged, which may block your connections (if so configured in the profile).

## 6.3. Virus & Spyware Protection

### Scanning type description mismatches between Scanning Report and user interface menus [66186]

The "Scanning type" line in the Scanning Report (HTML file) shows the type of the scan that created the report. The scan type description does not always match with the name of the scanning task as shown in the user interface menu.

- "Virus and spyware scan" (menu command) is shown as "Quick malware scan" in the report (note: the product help also uses both terms "Quick malware scan" and "Virus and malware scan" for describing this scan).
- "Rootkit scan" (menu command) is shown as "Quick rootkit scan" in the report.
- "Full computer scan" (menu command) is shown as "Full scan" in the report.

The information shown in the scanning report still applies to the scanning task that was executed from the user interface menu.

### Counters of scanned and clean files in Statistics not always correct [65977]

The Statistics page in the user interface displays the "Scanned files" and "Cleaned files" counters under the "Virus and spyware scanning" header. Sometimes these values do not correspond to the actual number of files that have been scanned or cleaned.

To find out how many files were actually scanned or cleaned, refer to the scanning report and the "Virus and spyware history" list.

### E-mail scanning remains active when real-time scanning is disabled [65735]

When the user disables real-time scanning from the product's user interface, the "Scan and remove viruses from e-mails" checkbox will be grayed out indicating that the e-mail scanning is also disabled. However, the e-mail scanning is active independently from the real-time scanning.

If you need to disable both real-time and e-mail scanning, clear the "Scan and remove viruses from e-mails" checkbox first and then the "Turn on real-time scanning" checkbox. Both features are disabled now. Note that you can select the "Unload" command from the system tray icon it to disable all the protection features.

 

### Multiple entries in “Virus and spyware history” log [65384]

When real-time scanning detects and automatically cleans an infected file on the system, two or more entries of the same file may appear in the “Virus and spyware history” log. An application or the operating system may try to open the same infected file multiple times, so detecting the infection may be logged multiple times. These extra entries in the log can be ignored.

### Files downloaded with MS Internet Explorer (IE) are reported as two files when scanned [65082]

When a file has been downloaded with MS Internet Explorer (IE) and then scanned with manual scanning, the number of scanned files may be reported two instead of one (as would be expected).

This occurs because IE attaches an alternative data stream (ADS) to the downloaded file. This ADS is invisible to the user, but the virus scan also scans all ADSes of files as they may contain malware, and the scanned ADSes are added to the scanned files counter.

### Deleted or quarantined file may remain visible [64229]

Sometimes after the product has reported that it successfully removed an infected file, the file may still remain visible in Windows Explorer for a while.

This occurs because the file may be opened by another application or the operating system. The file disappears when the other application or the operating system closes the file. If this does not happen, the file is removed after the computer is restarted.

### Command-line scan may not start while another scan is in progress, with unclear error message [61247]

When scanning the system is in progress (e.g. a task “Full computer scan” is running), any attempt to start a command-line scanning task (with fsav.exe) may fail with error messages "Error: Cannot start the scan, try again" and "Error: Unknown error".

Certain portions of the scanning task cannot be run simultaneously. As a workaround, try to start another scan a few minutes later.

### Automatically deleted spyware and riskware not correctly shown in scanning report [61155]

When the manual scanning is set to “Delete the files”, spyware and riskware removed by manual or scheduled scanning tasks are not shown as “deleted” in the scanning report. The malware is removed from the computer, but the scanning report does not show this. This happens with the “Delete the files” action only, for example, with the “Clean the files” action, malware is disinfected or quarantined, and this shows correctly in the scanning report.

### Quarantining action only available for files on local hard disk [61034]

The quarantining action for infected files is only designed to work for files on the local hard disk.  Files on removable media (e.g. USB memory sticks) or remote (network) drives cannot be quarantined. For example, when manual scanning setting has been set to “Quarantine the files” and an infected file is scanned on a USB memory stick, no action is done to the file. To remove an infected file from removable media or remote drives, select the “Delete the files” action or remove the files manually.

 

### Infected files from restored folder may not get detected [59875]

If a previously deleted folder (as moved to “Recycle Bin”, not permanently deleted) contained infected files, and you restore the whole folder, the infected files may remain undetected.

This may occur because restoring a folder from “Recycle Bin” is implemented as a simple folder-rename operation if the folder is located on the same hard disk as the “Recycle Bin” folder. Real-time scanning does not scan files during the folder rename operations because it would make renaming files and folders slower. If you try to open or run the infected file from the restored folder, the product detects and blocks it, so malware cannot activate on the computer.

### Progress bar does not account for files scanned inside archives [59503]

A progress bar is displayed for manual scanning tasks that shows how much of the scanning task has been completed. Files scanned as packed inside archive files (e.g. zip) are not taken into account in the progress indicator. For example, if the scanning target includes two equally large zip archives, the progress bar will remain at 0% until the first of the archives has been scanned completely, and then jump to 50%. It will remain at 50% and jump directly to 100% when the scanning of the second archive file has been completed. If the scanning target includes a single archive file only, the progress bar will remain at 0% until the scan is completed.

### Infected files dragged and dropped from VMware host not detected [59093]

If the product is running inside a virtual machine, under the VMware for Workstations product, when a folder with infected files is dragged and dropped from the host computer to the VMware guest computer with the product, infected files that were copied to the virtual machine may not be detected by real-time scanning. This only happens when complete folders are copied to the virtual machine: when individual files are copied, real-time scanning detects the infected files.

Attempts to open or execute these infected files are detected and blocked by real-time scanning, so malware cannot activate on the computer.

### “Quick Malware Scan” reports infections as single items [58869]

When a malware is detected on the system by the “Quick Malware Scan” command, all infected objects (files, registry settings) related to this malware are reported as a single infected “System Infection” item. If the same malware is detected by the “Scan all hard disks” or “Scan target” commands, all the detected infected files are be reported as separate infected items.

This behavior is by design, as the “Quick Malware Scan” task is designed to make the removal of system infections easier to the user, so all the detected objects are removed or quarantined in a single step.

### Only a single file can be scanned when its shortcut is right-clicked [57568]

In Windows Explorer, the user may select multiple files, then right-click and scan the selected files from the right-click menu. If one of the selected files is a shortcut file to another file, and mouse is clicked on top of this shortcut, the right-click menu only allows the single file (to which the shortcut points) to be scanned, and the other selected files will not be scanned.

 

### Windows Vista: Real-time scanning does not scan files being backed up with the block-level backup method [56759]

When the hard disks are being backed up with the block-level backup method, the backup process does not back up the disk file by file, but reads the disk “raw”, sector by sector. Because of this, real time scanning does not scan the files as they are being backed up, and infected files may end up in the backup store. Similarly, the infected files may not be detected by real-time scanning when they are restored from the backup.

On Windows Vista, the block-level backup method is used if the user chooses to use the “Complete PC Backup” option. If the "Back Up Files” option is selected, the chosen files/folders are backed up file by file: in this case, real-time scanning blocks access to the infected files, and the backup process is aborted.

### Real-time scanning may interfere with System Restore [56695]

If the system contains a virus or spyware or they have been present on the system previously, the System Restore feature may fail to restore the system to a previous restore point. This may happen because the real-time scanning blocks the access to infected files. This happens if System Restore tries to delete an existing infected file, and when it tries to restore an infected file from the previous restore point. As System Restore cannot open the infected file, it treats this as a fatal error and aborts the restore process.

As a workaround, disable real-time scanning before starting the restore process, and turn it back on after its completion.

More information about how System Restore is affected by Anti-Virus products is available in Microsoft’s KB article at http://support.microsoft.com/kb/831829.

### Command-line scanner and scheduled scanning tasks may find more spyware than scanning tasks executed from user interface [55119]

In some cases, the command-line scanner and scheduled scans may find more spyware than manual scanning task that is executed from user interface (UI). These two scanning methods are related as scheduled scanning tasks use the command-line scanner (fsav.exe).

Scheduled scans are run under a different user account (the Local System account, as opposed to the currently logged on user account that is used when the scanning task is started from the UI). The Local System account has access to some folders that the user cannot access, like the System Restore folder.

### Windows Vista: Removal of malware detected while running backup fails [54736]

If the computer contains infected files and these files are backed up using Vista’s the "Back Up Files” option in the “Back up your computer” feature, real-time scanning detects the infected files during the backup process and blocks access to them. As a result, the backup cannot complete. This behavior is by design, as real-time scanning prevents access to the infected files as it should.

When real-time scanning detects the infection, the product asks what to do with the infected file from the user. However, the product does not perform the action that the user selects. This issue will be fixed in a subsequent release.

To remove the infection, scan the infected file again with manual scanning. Then run the backup again.

 

### Restricted user cannot remove malware [54576]

If a user is logged on to the computer with a restricted account and the folder that the user scans does not include write permissions to restricted users, the user cannot remove malware if infected files are found in the folder.

For example, if the infected files are under the system folders (e.g. "C:\WINDOWS") or Program Files folders (e.g. “C:\Program Files"), restricted users cannot remove them. Removal succeeds if the files are under the user's own folder.

This behavior is by design, to make sure that restricted users cannot remove important system files: sometimes false alarms may occur, and some software, especially those categorized as "riskware" by the product, may have legitimate uses and should not be removed by users who do not have administrator permissions.

To remove malware from restricted folders, log on to the computer with an account that has Administrators’ privileges.

### When a virus is detected, Vista prompts for administrator permission [54418]

When real-time scanning detects malware in a file that is being accessed by the operating system, the operating system may show a message “Destination Folder Access Denied: You’ll need to provide administrator permissions to copy this file”. If the user provides permissions to complete the operation, the operating system still cannot access the file and the user is asked to retry. This can happen, for example, when the user attempts to unpack a compressed (zipped) folder that contains an infected file.

This behavior is by design. When real-time scanning detects an infected file, it blocks access to the file completely, including the access from the operating system components, to make sure that malicious programs do not activate on the system. When Vista cannot access a file that it tries to open, it incorrectly assumes that the operation failed because the user does not have enough privileges to access the file, and shows the described message.

### Automatic actions for viruses also used for suspicious items [53064]

When the action setting for viruses for manual scanning has been set to Delete, Quarantine or Rename automatically, and suspicious items (files that are hidden by a rootkit but not found infected by known malware) are found by rootkit scanning, all detected suspicious items are either deleted or renamed, based on the following list:

- Action for viruses = Delete automatically: suspicious items are deleted
- Action for viruses = Quarantine automatically: suspicious items are deleted
- Action for viruses = Rename automatically: suspicious items are renamed

Note that when "Quarantine automatically" is selected, suspicious items are deleted and not quarantined, as quarantining suspicious items is not available in the product currently.

In some situations, this behavior can be dangerous, for example, if a rootkit hides important operating system or application binaries. However, this is not a likely scenario, as hiding such binaries would cause the operating system malfunction in any case.

If the automatic action for viruses is "Disinfect automatically", suspicious items are not handled (action is reported as "failed" in the scanning report).

With the default "Ask what to do" setting, the user can select the action on suspicious items. If the user chooses to select the actions automatically in Scan Wizard, no actions are done on suspicious items.

 

### Scanning report created inconsistently with real-time scanning detections [52903]

After manual scanning, a scanning report (fsav_rep.htm) is created and viewable by clicking the “View virus and spyware history” link on the user interface (Virus and spyware scanning page). If real-time scanning detects an infected file and the user selects an action on the file (quarantine, disinfect or delete), the scanning report is created as well. However, the scanning report is not created if the user selects no action on the infected file.

### Malware/spyware/riskware removal may result in error messages about failures to remove, or inconsistent removal actions may be reported [65349, 65257, 50979]

If malware/spyware/riskware is on the system already (malware/spyware/riskware is active), the scanning report may contain multiple infected items. These reported items may be a part of the same malware/spyware/riskware.

When this malware/spyware/riskware is removed, the report may show an error message for some items, or the action “None” is shown and these items are not reported as “cleaned”, “deleted” or “quarantined”.

In some cases, the scanning report (HTML file), “Scan Wizard”, and “Virus and spyware history” contain inconsistencies. Scan Wizard and the history may report malware as quarantined, while the scanning report shows that it was deleted.

This may happen because the removal of one malware/spyware/riskware component also removes some other components before their turn. For example, when the user selects “Perform full computer check” to an infected computer, the report shows error messages or the action “None” for items that were originally detected as infected, but did not exist anymore when the product tried to remove them.

Another scenario is where the “Quick malware scan” finds multiple similarly named malware/spyware/riskware items. When the first item is quarantined, the second one is quarantined automatically, which quarantines all files of both malware/spyware/riskware under a single item. The scanning report (HTML file) may show the second item as deleted and not quarantined, while in fact it is quarantined as part of the first item.

To make sure that the malware/spyware/riskware was removed correctly and that above described inconsistencies in scanning reports do not indicate a real problem, restart the computer after the removal operation and run the “Quick malware scan” task again. If it does not detect any malware, the removal has been successful.

### Excluded filename extensions ignored for scans inside archives [50408]

Files with particular file name extensions can be configured to be excluded from scanning. This exclusion is not applied to files which are scanned inside archive files. For example, if a zip archive contains .mp3 files, the files are scanned even if the .mp3 extension is excluded from scanning.

### Viruses detected during ntbackup are not quarantined [47300]

If real-time scanning is set to “Quarantine automatically” for viruses and viruses are found while ntbackup tries to back up infected files, real-time scanning blocks the access to infected files, but files are not quarantined.

### Real-time scanning causes hangings in Visual C++ 6.0 [28849, 28402]

Real-time scanning may cause the computer to hang for a short period. To solve this issue, add the following registry key:

[HKEY_LOCAL_MACHINE\Software\Data Fellows\F-Secure\GKH2]

“NoLongPathExpand”=dword:00000001

Due to a problem with Microsoft Visual C++ 6.0 SP5 (or older) IDE saving a file that may cause the product to fail, Microsoft advises that the you should try to save the file again. This problem is fixed in Microsoft Visual Studio 6 service pack 6. For more information, see http://support.microsoft.com/default.aspx?kbid=822856.

Real-time protection causes some overhead on file I/O every time, which may have issues with time-critical file operations such as creating CD-R/CD-RW images.

## 6.4. DeepGuard

### DeepGuard Advanced Process Monitoring might cause problems with anti-cheating systems for online games and software genuineness checking

Enhanced process monitoring, which is on by default, may conflict with some 3rd party tampering protection systems, for example anti-cheating systems for online games and software genuineness checking systems. If you notice any of the described compatibility issues, please report them to our support.

You can turn Advanced Process Monitoring on and off in the Advanced settings of the DeepGuard page.

### DeepGuard limited functionality in Vista 64-bit without Service Packs [57225]

DeepGuard has limited functionality in 64-bit Windows Vista without any installed Service Packs. To fully enable DeepGuard functionality, install Windows Vista Service Pack 1 or later.

## 6.5. E-mail Scanning

### TLS- and SSL-encrypted e-mail protocols not supported [44173, 44869, 54496, 55285, 89415]

E-mail scanning works only with unencrypted e-mails using protocols POP3, IMAP or SMTP.

Scanning e-mails that are encrypted with Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols is not supported. When TLS and SSL protocols are used, e-mail scanning may either block all e-mails or fail to scan them. Turn off e-mail scanning if you use either TLS or SSL protocols for secure e-mail transmissions.

If E-mail scanning is configured to listen to a port which is used by TLS- or SSL- encrypted e-mail, the traffic is blocked completely even when e-mail scanning is turned off [89415]. To work around the problem, reconfigure E-mail scanning to a standard unencrypted port (110) or, if the later is used, to any unused port.

## 6.6. Web Traffic Scanning

### Web Traffic Scanning always scans inside archives [49120]

Web Traffic Scanning scan inside archives every time, whether this is turned off from the user interface or not.

### Web Traffic Scanning might cause problems with some client server applications

Some cases have been reported in which Web Traffic Scanning does not work with some client & server applications. We are currently investigating this and would like to receive more information about similar cases.

Turn off Web Traffic Scanning if it causes problems or uninstall it completely. Some applications that have been reported to be problematic:

- Web Traffic Scanning blocks IBM Open Query Application [51957]
- Web Traffic Scanning conflicts with surf-lock2 [56405]
- Enovia VPM does not work with Web Traffic Scanning [56943]
- Web Traffic Scanning not working with Oracle [58072]

### Web Traffic Scanning might have interoperability problems with 3rd party software that uses LSP technology

Web Traffic Scanning may be interoperable with other software that uses LSP technology. Some web pages may be loaded incorrectly or the network may be missing completely. In this case, either turn off or uninstall Web Traffic Scanning or the 3rd part software. Some 3rd software may work even when you disable the LSP functionality. For details, see the 3rd party software manual.

### Some malware is not detected by Web Traffic Scanning [58557]

Some types of malware are not detected by Web Traffic Scanning, but real-time scanning detects them. These are due to the optimized scanning options for Web Traffic Scanning.

## 6.7. E-mail filtering

### Windows Mail (on Vista) loses focus when sending/receiving emails [54118]

When Widows Mail sends or receives e-mails and e-mail filtering turned on, the application loses focus. Any window that was behind Windows Mail pops up in front and you cannot select any menus in Windows Mail. After e-mails have been sent and received, you can use Windows Mail again normally by selecting it from the Windows task bar to get it on top again.

If you receive or send a lot of e-mails at the same time and you need to access Windows Mail, you can cancel the operation temporarily from the send/receive window.

### E-mail filtering might be affected by low system resources [54285]

If the system is low on resources, spam e-mails may not be filtered properly or at all. The e-mail filtering button in Windows Mail (or Outlook Express) may not be shown either. This happens quite rarely and mostly in older machines that are very close to the minimum system requirements. If you encounter this issue, close some applications or restart your

 

computer. Consider upgrading the hardware or configuring the system, possibly by removing some software to increase performance.

### Windows Live Mail is not supported

In this release, e-mail filtering does not support Windows Live Mail.

## 6.8. Browsing Protection

### Disabling Browser Protection requires open browsers to be closed in order to be affected

If you have browser windows open and you disable Browsing Protection, the change affects open browsers after you close and start them again.

### Report dialog not shown in block page

The report button on the Browsing Protection toolbar does not work in the block page.

## 6.9. Software Updater

### Software Updater does not notify the user about its activity

The installation of missing updates starts according to schedule (defined in profile) and runs in the background that may slow down the usual work. However, the product does not display any visual notification about and does not allow postponing this activity.

### Software Updater does not automatically install updates not signed by trusted authority

Some updates, for example for Notepad++, WinZip, 7-Zip, are released unsigned. Software Updater does not automatically install unsigned updates and reports the installation error to the portal, code 10, “There is no signature”. Administrator can install such updates using selective installation from portal: at Software updates page choose ‘Install missing updates’ command.

### Inconsistent approach for status regarding Software Updater vs. other components [89374]

If the user turns off Software Updater, F-secure system tray icon and gadget colors do not notify the user about disabled security functions.

### Installation of some updates can hang

Installation of updates is running under local system account without user interaction. In rare case, installation can hang because of asking some user’s prompt or handling an error. Such a hanging installation is cancelled after the timeout period, which is 4 hours by default. After this happens, the batch installation continues skipping the problematic patch / update. Software Updater reports the installation error to the portal, code 11, “Installation hung up”.

To forcibly retry the installation of the problematic update, use selective installation from portal.

# 7. Contact Information and Feedback

We look forward to hear your comments and feedback on the product functionality, usability and performance.

Please report any technical issues through the F-Secure support web site: http://support.f-secure.com

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 PSB Workstation Security, right-click on “Support tool”, select Run as and finally select to run the program as administrator.
- In Windows 7 and Vista, select Start | All Programs | F-Secure PSB Workstation Security, right-click on “Support tool” and select Run as administrator.
- In Windows 8, right-click on “Support Tool” application in Windows Store and use “Run as Administrator” option.