

# RELEASE NOTES

## F-Secure PSB Workstation Security - Release To Manufacturing (9.00 build 149)

### 1. General

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

#### What's in This File

- Installation and System Requirements
- Product Contents
- New Features
- Fixed Issues
- Known Issues
- Contact Information and Feedback

### 2. Installation and System Requirements

#### 2.1. Operating systems supported

The supported operating systems for installing the product are:

- Windows XP 32-bit: Home, Professional and Media Center editions. Service Pack 2 or newer.
- Windows Vista 32-bit and 64-bit: All editions, all Service Packs.
- Windows 7 32-bit and 64-bit: All editions.

#### 2.2. System requirements

The system requirements for the product are:

##### Microsoft Windows 7 and Vista

- Processor: Intel Pentium 4 2GHz or higher
- Memory: 1GB or more
- Disk space: 800 MB free HD space (500 MB for Anti-virus only)
- Display: 16-bit or more (65000 colors)

- Internet Connection: An Internet connection is required in order to validate your subscription and receive updates

## Microsoft Windows XP

- Processor: Intel Pentium III 1Gz or higher
- Memory: 512 MB or more
- Operating System: Microsoft Windows XP SP2 or newer
- Disk space: 800MB free HD space (500 MB for Anti-virus only)
- Display: 16-bit or more (65000 colors)
- Internet Connection: An Internet connection is required in order to validate your subscription and receive updates

## 3. Product Contents

This product enables you to install:

- Virus & Spy Protection with Virus protection, Anti-spyware, Email Scanning and Web Traffic Scanning for viruses, Blacklight scanning for hidden malware and the proactive 0-day protection technology DeepGuard™.
- Firewall, Application Control, Intrusion Prevention and Dial-up Control.
- E-mail filtering with protection against spam and phishing.
- Automatic updates, enabling you to keep both the databases and the software up-to-date against the latest threats.
- Browsing Protection, helping you protect your personal information which you may sometimes have to enter on the Internet when, for example subscribing to newsletters, joining web communities or buying something online.

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

## 4. New Features

New features since the release of F-Secure PSB Workstation Security 4.0 include:

- **Windows 7 support**

The product can be natively installed on Windows 7.

- **New user interface**

The look and feel of the whole user interface has been renewed, and the main user interface has been completely redesigned. It simplifies many of the functions that the

user can perform. By reorganizing the interface into more logical areas, the user is able to perform related actions more easily.

Similarly, the design of the advanced settings has been restructured into more logical areas.

- **Automatic removal of malware**

The user is no longer prompted for actions when malware is found. Instead malware is automatically removed and the user is notified of this. This behavior can be configured in “Settings - Virus and spyware scanning”. There are now only two available options when virus or spyware is found:

- o If unclear, ask me
- o Always ask me

- **Action taken when scanning viruses and spyware is unified**

Only one decision about the treatment of malware is required. This affects both manual scans and scheduled scans.

- **Removal of Virus and spyware security levels**

There are no longer any Virus and spyware security levels. All settings can be configured individually.

- **Refined infection cleaning dialog**

The dialog which is presented when a virus is being removed has been refined so it's possible to minimize it and use the computer while the infection is being cleaned. The look and feel of the dialog has also been updated, and an accurate progress bar has been added.

- **Virus and spyware history**

From Virus and spyware history, the user can see what has been done to viruses and spyware that have been found on their computer.

- **Scanning performance improvements without sacrificing security**

F-Secure's multi-engine protection has been upgraded to offer faster malware scanning and smaller memory usage while keeping the detection rate on highest possible level.

- **Browsing Protection**

Browsing Protection protects users from web-based malicious exploits and stops malware at the first point of infection. All malicious, exploit-hosting URLs it detects are automatically reported back to F-Secure's Real-time Protection Network, which helps our Security Labs discover new exploits on the Internet and react to protect all our existing customers. Browsing Protection also protects against rogue web sites, by showing the rating of sites directly in the browser.

The Browsing Protection feature can be configured in “Settings - Internet - Browsing Protection”.

Browsing Protection is supported when using Internet Explorer 6 or newer, or Firefox 2 or newer. Other browsers are not supported at this time.

- **DeepGuard no longer dependent on Real-Time Scanning**

DeepGuard (previously sometimes referred to as System Control) can now be enabled even when Real-Time Scanning is disabled.

- **DeepGuard Advanced Process Monitoring**

Many Trojans and malware try to infect the user's browser to steal information like passwords, bank credentials or even money from the user's online banking session. DeepGuard has been extended to provide protection against these threats. This can be configured in "Settings - Computer - DeepGuard - Use advanced process monitoring". Advanced Process Monitoring also offers:

- o **protection against common browsing control commands**

- o DeepGuard offers protection against controlling browser with OLE and DDE commands.

- o **protection against stopping of F-Secure services**

- o DeepGuard will ask for authorizing the stopping of F-Secure services.

- **Limited amount of DeepGuard block dialogs per application**

Some malware launchers can launch the same malware an infinite amount of times, which from now on only results in a maximum of 5 blocked dialogs. After this, the application is blocked silently. At reboot, the counter is reset.

- **Fewer Application Control prompts**

Application Control now uses the Real-time Protection Network to reduce the amount of prompts when trusted applications try to connect to the Internet.

- **Boot-up optimization**

Some components that are active during the boot-up phase have been re-designed to be less CPU intensive. This results in faster boot-up time.

- **Several processes removed**

The functionality of the following processes has been merged into other processes: FSMB32.EXE, FSGUIDLL.EXE, FCH32.EXE, FAMEH32.EXE, fsaua.exe, fsus.exe, and fsqh.exe.

One new process, FSHDLL32.EXE (and FSHDLL64.EXE on 64-bit operating systems), has been created for hosting some of the functionality that the above processes used to offer.

This frees up memory and reduces the total thread count. The end result is 6 processes less compared to the previous release.

- **Dial-up Control is disabled by default**

Dial-up Control is now disabled by default. It can still be enabled through the "Settings - Network connections - Dial-up Control".

- **Participating in Real-time Protection Network**

By participating in the Real-time Protection Network, the user contributes anonymous data to further improve the service.

- **Improved interoperability with Web Traffic Scanning**

Web Traffic Scanning now interferes less with 3<sup>rd</sup> party applications that send or receive data over the network. Web Traffic Scanning no longer scans the traffic of all networking applications, and only the following web browsers are supported by the Web Traffic Scanning feature:

- Microsoft Internet Explorer
- Mozilla Firefox
- Google Chrome
- Opera
- **LSP on-demand installation**

The F-Secure LSP (Layered Service Provider) is now only hooked into the TCP/IP stack if Web Traffic Scanning is enabled. This reduces the likelihood of incompatibility issues with other software utilizing LSP technology when Web Traffic Scanning is disabled.
- **AUA Support for PAC and WPAD**

Support for automatic configuration of HTTP Proxy using PAC (Proxy Auto Configuration) scripts or WPAD (Web Proxy Auto-Discovery) has been added.

## 5. Known Issues

### 5.1. Installation and Uninstallation

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

When the product is installed, a “restore point” will be created prior to installation, making it possible to use the System Restore feature of Windows to restore the system to the state of the system before installing the product.

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

These remaining files will cause problems when the product is reinstalled to the system again. Installation will be partly successful, but installing the downloaded updates will fail, and the product will never achieve a completed installation state.

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

Workaround: 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 ensure successful installation.

## **Some localizations (e.g. Estonian) can only be installed when the proper system codepage is selected**

This problem can be worked around by changing the OS setting “language for non-Unicode programs”.

## **Application control might warn about lh8run.exe during channel upgrade from earlier versions**

Application control might show a warning about the F-Secure process “lh8run.exe” during channel upgrade from an earlier version. This would be visible 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**

In case of an upgrade, some databases and engines used by the previous version might not be needed anymore. These are still visible in “Settings – Other settings – Downloads”, marked as “Not Installed”. This is normal, and after 7 days they will be automatically removed.

## **Inconsistent Post Installation dialog information regarding updates**

During the installation of certain updates, such as customizations or hot-fixes, it is possible that the Post Installation dialog will show inconsistent information about which update is currently being installed. It might for example change from saying “Installing update 3/10” to “Installing update 10/10” and then back to “Installing update 4/10”. This is only a visual problem, and the situation recovers shortly by itself to show the real status.

## **Guest account users will not be notified of major product upgrades**

If an upgrade is available, it will not show to users who do not have permission to carry out the installation. The upgrade will be listed on the Downloads page in Settings, but it will not prompt to install it unless you are logged in to a Windows account with high enough permissions to complete the installation.

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

In case 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 might be slow to finish. This is because the internet browser is trying to resolve the proxy settings, and the Automatic Update Agent waits for this to finish.

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

### **Firewall in Cisco VPN Client does not work with F-Secure Internet Security [52211]**

Cisco VPN Client has a built-in stateful firewall, which is not compatible with F-Secure Internet Security. If Cisco VPN Client is installed before Internet Security, the sidegrade component

disables the firewall in Cisco VPN Client. However, in some cases it might be that the side-grade cannot identify a new version of Cisco VPN Client. In that case you can disable the integrated firewall manually.

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

The Base Filtering Engine service on Vista platforms must not be disabled. F-Secure Firewall fails to function without it.

## **5.3. Virus & Spy 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 this report applies to. The scan type description does not always exactly match with the name of the scanning task shown in the user interface menu used for starting the scan.

- "Virus and spyware scan" (menu command) is shown as "Quick malware scan" in the report (note: help also uses both terms "Quick malware scan" and "Virus and malware scan" for describing the same type of scan; also the present release notes use the term "Quick malware 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.

This is just a cosmetic issue; the information shown in the scanning report still applies to the scanning task that was executed from the menu.

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

The Statistics page in the product's user interface displays the "Scanned files" and "Cleaned files" counters under the "Virus and spyware scanning" header. These counters are not always updated correctly, so the values shown do not correspond to the actual number of files 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, indicating that e-mail scanning is also disabled. In fact, e-mail scanning remains active independently from real-time scanning.

Workaround: in case it is required to disable both real-time and e-mail scanning, first uncheck the "Scan and remove viruses from e-mails" checkbox, and only then uncheck the "Turn on real-time scanning" checkbox. Now both features will be disabled. Note that from the product's system tray icon it is also possible to select the "Unload" command that will disable all the product's protection features.

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

When real-time scanning detects an infected file on the system and it is automatically cleaned, two or more entries of the same file may appear in the “Virus and spyware history” log. This happens because an application or the operating system may try to open the same infected file multiple times, and the event of detecting the infection is logged multiple times. The 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 behavior is by design. It occurs because IE attaches an alternative data stream (ADS) to the downloaded file. This ADS is invisible to the user, but the scanner also scans all ADSes of files because 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 of a successful removal of 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 will become invisible once the other application or the operating system has closed the file. If this does not happen, the file will be removed after restarting the computer the latest.

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

When scanning the system is already in progress (e.g. a task “Full computer scan” is running), 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”.

Due to the design of scanning the system, certain portions of the scanning task cannot be run simultaneously. As a workaround, try scanning a few minutes later.

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

When the manual scanning action setting 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 actually removed from the computer, but the scanning report does not indicate the action taken. The problem only applies to the “Delete the files” action, for example, with the “Clean the files” action, malware is disinfected or quarantined, and this is indicated 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 will be done with 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]**

When a previously deleted folder (as moved to “Recycle Bin”, not permanently deleted) contained infected files, and the whole folder is being restored, the infected files may remain undetected when being restored.

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 upon folder rename operations because this would make such operations much slower. The infected files will be detected and blocked in any case when being opened or executed from the restored folder, so malware cannot activate on the computer regardless of this problem.

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

A progress bar is shown for manual scanning tasks to indicate the portion of scanning task 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 then the progress bar will remain at 0% until the first of the archives has been completely scanned, at which point the progress bar will jump to 50%. It will remain at 50% and will 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 then the progress bar will remain at 0% until the scan is completed.

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

This problem is specific to the product 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 Anti-Virus product, infected files thus copied to the virtual machine may not get detected by real-time scanning. This only happens when complete folders are copied to the virtual machine: when individual files are copied then real-time scanning detects the infected files.

Attempts to open or execute the infected files previously copied to the virtual machine will get detected and blocked by real-time scanning, so malware cannot activate on the computer regardless of this problem.

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

When a malware is detected on the system by the “Quick Malware Scan” command then all infected objects (files, registry settings) related to this malware will be reported as a single infected “System Infection” item. If the same malware is detected by the “Scan all hard disks” or “Scan target” commands then all the detected infected files will 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: all the detected objects will be 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 the mouse, and scan the selected files from the right-click menu. In case 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 will not back up the disk file by file, but will read the disk "raw", sector by sector. Because of this, real time scanning will not scan the files as they are being backed up, and infected files will end up in the backup store. Similarly, the infected files may not be detected by real-time scanning when they are restored from 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 will be backed up file by file: in this case, real-time scanning will block access to the infected files, and the backup process will be aborted.

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

In case virus or spyware infections are present or have previously been present on the system, the System Restore feature may fail to restore the system to a previous restore point. This may happen because the real-time scanning feature will block any access to infected files. This applies both in case System Restore tries to delete an existing infected file, and in case it tries to restore an infected file from the previous restore point. As System Restore fails to open the infected file, it will treat this error condition as a fatal error and will abort the restore process.

As a workaround, disable real-time scanning before starting the restore process, and re-enable it 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 executed from user interface (UI). These two scanning methods are related because the scheduled scanning tasks actually use the command-line scanner (fsav.exe). The reason for this is that the scheduled scans run under a different user account (Local System, as opposed to the currently logged on user account used for UI-started scanning tasks). The Local System account has access to some folders where the user does not have access, like the System Restore folder.

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

If there are infected files on the computer and these files are being backed up using Vista's "Back up your computer" feature using the "Back Up Files" option, real-time scanning will detect the infected files during the backup process and will block access to them. As a result, the

backup operation fails. This behavior is by design, as real-time scanning needs to prevent access to the infected files.

As a result of real-time scanning detection of the infection, the user is prompted for an action on the infected file. When the user selects an action to disinfect, delete or quarantine the file, the action will fail. This is a bug in the product and will be fixed in a subsequent release.

Workaround: rescan the infected file with a manual scanning operation and select an appropriate action to remove the infection. Then run backup again.

### **Restricted user cannot remove malware [54576]**

Malware removal fails if the scanning and removal task is run by a user who is logged on to the computer under a restricted account, and the folder with the infected files does not include write permissions to restricted users. For example, if the infected files are under the system folders (e.g. "C:\WINDOWS") or Program Files folders (e.g. "C:\Program Files") then restricted users will not be able to remove them. Removal will succeed 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 be able to remove all malware, log on to the computer under an account that belongs to the Administrators group.

### **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 an error message "Destination Folder Access Denied: You'll need to provide administrator permissions to copy this file". After the user decides to grant administrator permissions for completing the operation, the operation to access the file still fails and the user is asked to retry. A typical scenario for this error message to appear is 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 this file to any process on the system, including operating system components. Blocking access to the infected files is necessary to make sure that malicious programs will not activate on the system. When Vista gets an "access denied" error from the file open operation, it incorrectly assumes that the operation failed because the user does not have enough privileges to access the file, and will show the described error 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 then all the suspicious items detected will either be deleted or renamed also, according to the following list:

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

Note that as noted above, "Quarantine automatically" will result in suspicious items to be deleted instead of quarantining, as quarantining of suspicious items is currently not an available feature in the product.

In some situations, this behavior can be dangerous, for example, in case a rootkit would hide important operating system or application binaries. This is however not a likely scenario, as hiding such binaries would make the operating system or the application dysfunctional anyway.

In case the automatic action for viruses is "Disinfect automatically" then no action will be done on suspicious items (action will be reported as "failed" in scanning report in this case).

With the default action setting for manual scanning, "Ask what to do", the user will be able to select an appropriate action on suspicious items. If the user chooses to select the actions automatically in Scan Wizard then no actions will be done on suspicious items.

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

After execution of a manual scanning task, a scanning report (fsav\_rep.htm) is always created, viewable by clicking on the "View virus and spyware history" link on the product's user interface (Virus and spyware scanning page). In case real-time scanning detects an infected file and the user selects to execute some action on the infected file (quarantine, disinfect or delete), the scanning report will also be created. However, the scanning report will not be created if the user selects to do 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 has been already installed on the system (the malware/spyware/riskware is active) then its removal may result in multiple infected items to be reported. These different reported items may be part of the same malware/spyware/riskware.

When this malware/spyware/riskware is being removed then the removal may otherwise succeed, but for some reported items, either error messages are shown, or action "None" is shown and these items are not reported as "cleaned", "deleted" or "quarantined".

In some cases, there are inconsistencies between what the "Scan Wizard", "Virus and spyware history" and the scanning report (HTML file) report. Scan Wizard and the history may report the malware as quarantined, while scanning report shows it as deleted.

This behavior may occur because the removal of one malware/spyware/riskware component also removes some other components already before the removal of the other components is executed. A typical scenario where this happens is when the "Perform full computer check" scan is executed in an infected computer. As a result, error messages or action "None" are shown 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 discovered item is quarantined, the second one will be quarantined automatically, resulting in all files of both malware/spyware/riskware being quarantined under a single item. The scanning report (HTML file) may show the second item as deleted not quarantined, while in fact it had been quarantined as part of the first item.

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

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

The product may be configured to exclude files with particular name extensions to be excluded from scanning. This exclusion is not applied to files 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 ntbakup are not quarantined [47300]**

In case the “Quarantine automatically” action on viruses is selected for real-time scanning and the viruses are found while ntbakup is trying to back up the infected files, real-time scanning will properly block access to the infected files, but the files will not be 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 work around this problem please add the following registry key “HKEY\_LOCAL\_MACHINE\Software\Data Fellows\F-Secure\GKH2: NoLongPathExpand (REG\_DWORD) = 0x1”.

Due to a problem with Microsoft Visual C++ 6.0 SP5 (or older) IDE saving a file with that product may fail, Microsoft advises that the operation should be tried again, in case of a failed save operation. 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 always causes some overhead on file I/O, which can cause problems for time-critical file operations such as creating CD-R/CD-RW images.

## **5.4. DeepGuard**

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

It is possible that enhanced process monitoring, which is on by default, conflicts with some 3rd party tampering protection systems, e.g. anti-cheating systems for online games and software genuineness checking. In case you notice compatibility issues described above, please report them to our support.

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

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

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

## DeepGuard doesn't protect services in Windows 7 [65247]

When stopping a protected service from command line or from Services, DeepGuard fails to prompt about it. However, it still protects services from most malicious stop attempts. This problem only occurs in 32-bit operating systems.

## 5.5. E-mail Scanning

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

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

Scanning of e-mails encrypted with the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols is not supported. E-mail scanning may either block all e-mails or fail to scan the e-mails if the TLS and SSL protocols are used. If you are using either of the above protocols for secure e-mail transmissions then e-mail scanning must be disabled.

## 5.6. Web Traffic Scanning

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

Web Traffic Scanning will always scan inside archives, independent on if 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 causes problems with some client & server applications. Investigations are ongoing and we are happy to receive more information about cases like this. Workaround is to turn off Web Traffic Scanning if the problem occurs or in worse case uninstall it. 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 might be interoperable with other software that uses LSP technology. This could result in incorrectly loaded web pages or totally missing network. In this case either Web Traffic Scanning or the 3<sup>rd</sup> part soft should be disabled/uninstalled. Some 3<sup>rd</sup> software might also work even if they don't have their LSP functionality enabled. For details see the manual of the 3<sup>rd</sup> party software.

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

Some types of malware are not detected by Web Traffic Scanning, but instead they are picked up by real-time scanner. These are due to the optimized scanning options for Web Traffic Scanning.

## **5.7. E-mail filtering**

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

When Windows mail is sending or receiving emails with E-mail filtering active it loses focus. Any window behind Windows mail pops up in front and you cannot select any menus in Windows mail. This is annoying but when sending / receiving has finished, you can use Windows mail again normally by first selecting it from the Windows task bar to get it on top again.

If you receive/send a lot of emails at the same time and need to access Windows mail during this, then cancel the sending / receiving temporarily from the send / receive window.

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

If the system becomes low on resources, the E-mail filtering might be one of the first applications in the system that is affected. In such a case, the spam emails might not be filtered properly or in worst case at all. The E-mail filtering button in Windows Mail (or Outlook Express) might not be shown as well. This is quite a rare condition and it is likely only to happen occasionally in older machines that are very close to the minimum system requirements. If this becomes a problem try closing some open applications or restarting your computer. If the problem persists consider upgrading the hardware or fine tuning the system by possible removing some of the installed software for more performance.

### **Windows Live Mail is not supported**

In this release Windows Live Mail is not supported by F-Secure E-mail filtering.

## **5.1. Browsing Protection**

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

If there are open browsers and the Browsing Protection feature is disabled, the change will only affect the open browser once it has been closed and restarted.

### **Report dialog not shown in block page**

The report button on the Browsing Protection toolbar will not function in the block page.

## **6. 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://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.