

F-Secure Anti-Virus for Servers

[Online Help](#)



"F-Secure" and the triangle symbol are registered trademarks of F-Secure Corporation and F-Secure product names and symbols/logos are either trademarks or registered trademarks of F-Secure Corporation. All product names referenced herein are trademarks or registered trademarks of their respective companies. F-Secure Corporation disclaims proprietary interest in the marks and names of others. Although F-Secure Corporation makes every effort to ensure that this information is accurate, F-Secure Corporation will not be liable for any errors or omission of facts contained herein. F-Secure Corporation reserves the right to modify specifications cited in this document without prior notice.

Companies, names and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of F-Secure Corporation.

This product may be covered by one or more F-Secure patents, including the following:

GB2353372 GB2366691 GB2366692 GB2366693 GB2367933 GB2368233
GB2374260

Copyright © 2008 F-Secure Corporation. All rights reserved.

Contents

Chapter 1	Getting Started	5
1.1	Options for Accessing the Product.....	6
1.1.1	Windows Start Menu	6
1.1.2	The System Tray Icon	6
1.1.3	The Windows Explorer Right-Click Menu	8
1.2	Using the Product for the First Time	9
1.2.1	Is the Product Active and Working Properly?	9
Chapter 2	Home	12
2.1	Home Tab	13
2.2	Security News	15
2.2.1	Security News Details.....	15
Chapter 3	Virus and Spy Protection	17
3.1	Basic Virus and Spy Protection.....	18
3.1.1	Virus and Spy Protection Level	19
3.1.2	Scan My Computer.....	20
3.1.3	Quarantined Items	21
3.2	Advanced Virus and Spy Protection.....	23
3.2.1	Real-time Scanning	24
3.2.2	Scheduled Scanning.....	37
3.2.3	Manual Scanning.....	38
3.3	Using Virus and Spy Protection	41
3.3.1	Removing Viruses and Spyware From Your Computer.....	41

3.3.2	Scanning Manually	43
3.3.3	Using The Scan Wizard.....	44
3.3.4	Removing Viruses And Spyware Manually.....	53
3.3.5	What if You Suspect You Have Found a New Malware?	55
3.3.6	Using System Control.....	56
Chapter 4	Automatic Updates	59
4.1	Basic Automatic Updates	60
4.2	Advanced Automatic Updates.....	62
4.2.1	Connection	63
4.2.2	HTTP Proxy.....	64
4.2.3	Downloads.....	65
Chapter 5	Glossary	66

1

GETTING STARTED

Using the Product for the First Time.....	9
Options for Accessing the Product	6

1.1 Options for Accessing the Product

There are several ways of accessing and using the product:


- Windows Start Menu
- The System Tray Icon
- The Windows Explorer Right-Click Menu


1.1.1 Windows Start Menu

To access basic operations, view manuals and web pages:


1. Open the Windows *Start* menu.
2. Go to the *All Programs* menu and the *F-Secure Anti-Virus for Servers* sub-menu.
3. Click *Open F-Secure Anti-Virus for Servers* to open it, or select another option from the sub-menu.

1.1.2 The System Tray Icon

You can use the system tray icon () in the Windows system tray (at the bottom right corner of your screen) to view the current status or access the right-click menu.

To open the main user interface, double-click the  icon with your left mouse button.

Pop-Up Menu

Click the  icon with the right mouse button to access the right-click menu with its list of common and frequently used operations. From the menu, you can open the main user interface or instantly scan for **viruses** and **spyware**.

To get a better understanding of each of the menu items, see the table below:

Selection	Description
Open	Opens the main user interface where you can view the status of all components and access advanced settings to modify your level of protection.
Unload / Reload	Unload installed components from memory. Sometimes this is necessary when installing some software, or doing performance-critical tasks. Do not leave your computer in this state for extended periods, as it is not protected. You can reload the products by selecting <i>Reload</i> . They will be automatically reloaded when you restart your computer.

Virus & Spy Protection

Scan target	Virus & Spy Protection scans a specific file or folder for viruses . Select the target directory or file and click OK to start the scan.
Scan hard drives	Virus & Spy Protection scans all files in your hard drives for viruses.
Quick spyware scan	Virus & Spy Protection scans the system only for spyware .
Quick rootkit scan	Virus & Spy Protection scans the system for rootkits and other hidden and suspicious items.
Perform full computer check	Virus & Spy Protection scans the computer for viruses, spyware and rootkits.
Show flyer list...	View all logged System Control events.

1.1.3 The Windows Explorer Right-Click Menu

You can scan disks, folders and files for **viruses** in Windows Explorer. To do this:


1. Place your mouse pointer on the disk, folder or file you want to scan, and right-click your mouse button.
2. From the right-click menu, select *Scan Folders for Viruses* (the selection may vary based on selected items). The *Scan Wizard* window appears and the scan starts.

If a virus is found, the Scan Wizard guides you through the disinfection stages.

1.2 Using the Product for the First Time

If you are using the product for the first time, you may want to check that the product is active and working properly.

1.2.1 Is the Product Active and Working Properly?







After you have finished the installation, check that the  icon is shown in your Windows system tray at the bottom right corner of your screen (as shown below).








Status Tooltip

Place your mouse over the icon to show the status tooltip. With the tooltip, you can instantly see the product status.

The icon may appear differently or not at all depending on the current status. See the list of icons and their meanings in the table below:

Icon	Status	What To Do
	The product is working properly. Your computer is protected.	Use your e-mail and browse the Internet as normal.
	Installation in progress. Your computer is not yet protected.	Wait for the installation to finish. The  icon will appear when the installation is complete.
	Download in progress.	Download progress is displayed on any download event, such as virus and spyware definition databases , software or security level updates.
	Error state. An error has occurred.	Place your mouse pointer over the  icon to see the reason for the error. If necessary, restart your computer.

Icon	Status	What To Do
	Warning. A protection feature has been disabled or your virus definitions are out of date. Your computer is not fully protected.	Place your mouse pointer over the  icon to see the status tooltip. Enable the feature that is currently disabled or check for updates. You may see this warning icon for example if you are defragmenting your hard drive, as some system functions by default cause all downloads to be suspended.
	Critical Warning State (flashing icon)	This icon is shown when the virus definitions have not been updated lately or the subscription expires. If your subscription expires, you need to renew the subscription to continue using the product.
	Unloaded. The product is deactivated and your computer is not protected.	Right-click the  icon and select <i>Reload</i> to activate the product.
No icon	The product is not installed or there was an error that prevented loading the program. Your computer is not protected.	Restart you computer and if the icon still does not appear, re-install the product.

2

HOME

Home Tab	13
Security News.....	15

2.1 Home Tab

The *Home* tab offers you a quick and detailed overview of your security settings and the status of all the installed components.

Selection	Description
Status	Shows the overall protection status.
Virus and Spy Protection	Shows the current Virus & Spy Protection level. Click Change... to change your Virus & Spy Protection level.
Last update check	Shows details of the last update. Click Check now to check for the latest updates.
Security News	Shows you whether you have any unread Security News available for you to read. The Security News is available only in English. Click View... to view Security News.
Advanced...	Opens the <i>Advanced Settings</i> window.



Depending on your subscription, some of the listed items may be unavailable.

2.2 Security News

On the Security News pages you can view reports on recent **virus** outbreaks and other security news. You can see the date and time of receiving each news item, followed by the subject of each report. The *Protection* column tells you whether your computer is protected against the virus in question or not.

To view the entire report, double-click a subject or select it and click **Details...** For more information, see “*Security News Details*”, 15.

To clear all Security News from the list, click **Clear All**.

If you wish to see a notification balloon each time you receive a news item, select the *Show notification balloon on system tray* check box.

2.2.1 Security News Details

In the Security News *Properties* window, you see a short article on the news item you selected. Below the article, you are told whether your computer is protected against the threat yet. There are four possible cases:

1. “*This computer is not protected yet. The update will be available soon in definitions version yyyy-mm-dd ##.*” There is no update available yet that could protect against this virus. A new update that protects against the virus will be available as soon as possible.
2. “*This computer is not protected against this virus. Update now...*” A new update is available but you do not have it yet. Click **Update now...** to update the product.
3. “*This computer is protected.*” Your definition updates protect you against this threat.
4. “*This computer can be protected only with the Internet Shield. Read the description for more information how to protect your computer.*” The malware reported in this news item uses network attacks to cause harm. The only way to protect your computer against it is by configuring Internet Shield to block its access to your computer.

Click **< Previous** and **Next >** browse other Security News items. Click **OK** to close the window.



3

VIRUS AND SPY PROTECTION

Basic Virus and Spy Protection	18
Advanced Virus and Spy Protection	23
Using Virus and Spy Protection	41

3.1 Basic Virus and Spy Protection

Virus and Spy Protection works automatically and in real-time in the background while you are using files in your computer or browsing Internet web sites.

Virus and Spy Protection:

- stops **malware**, including **viruses** and **spyware**, from attacking your computer by e-mail, removable media or downloaded content from the Internet.
- **quarantines** and removes viruses, spyware, and other malware that are installed on your computer
- blocks intrusive ad pop-ups and protects your system settings.
- detects riskware and quarantines or removes it

You can directly change the **protection level** and real-time scanning, e-mail scanning and scheduled scanning settings from the Virus and Spy Protection tab.

You can view your scanning reports and scan for viruses and spyware manually from the Virus and Spy Protection tab.

Selection	Description
Virus and Spy Protection	<p>Click Change... to change your Virus and Spy Protection level. Read the level description carefully before you select it.</p> <p>Protection levels are preconfigured security levels that determine how the product handles viruses and malware.</p> <p>If Virus and Spy Protection is disabled, your computer is vulnerable to virus attacks. For more information, see “<i>Virus and Spy Protection Level</i>”, 19.</p>
Real-time Scanning	<p><i>All files, Defined files or Disabled.</i> Shows you whether the real-time scan scans all files, all specified file types or whether it is disabled.</p>

If you disable real-time scanning, you can still scan the computer manually. For more information, see “*Scanning Manually*”, 43.

Click **Configure...** to change your real-time scanning settings.

Scheduled Scanning Shows the next time a scheduled scan starts if the scheduled scanning is enabled.

Click **Configure...** to set a scanning schedule.

Quarantined Items The number of items in the Quarantine repository.

Click **Configure...** to view and restore quarantined malware.

Scanning Report Displays the scanning report status.

Click **View...** to view the most recent scanning report.

Scan My Computer... Starts a manual scan for viruses, spyware, and other malware and suspicious items.

Advanced... Opens the *Virus protection* page of the *Advanced Settings* window. For more information, see “*Advanced Virus and Spy Protection*”, 23.

3.1.1 Virus and Spy Protection Level

Virus and Spy Protection levels allow you to change the level of protection according to your needs.

To change your Virus and Spy Protection level:

⇒ Go to the Virus and Spy Protection tab and click **Change....**

When you change the Virus and Spy Protection level, you can view the selected level description. Read the level description carefully before you select it.

You cannot change some Virus and Spy Protection settings if you use a *High* or *Normal* protection level. If you want to configure all settings manually, select *Custom* as your virus protection level..



If you change Virus and Spy Protection settings, all changes are saved for the currently selected protection level only.



IMPORTANT: Remember that if you disable *Virus and Spy Protection*, your computer is vulnerable to virus attacks.

3.1.2 Scan My Computer

When Virus and Spy Protection and the real-time scanning are enabled, your computer is protected. When you access any file, it is automatically scanned for **viruses**, **spyware** and other **malware**, and suspicious items.

If you suspect that your computer may contain malware or suspicious items, you can scan the computer manually

To start a manual scan:

1. Go to the Virus and Spy Protection tab and click **Scan my computer...**
2. Select one of the following options from the scan menu:
 - *Scan target* - scans a specific file or folder for malware and suspicious items.
 - *Scan hard drives* - scans all files in your hard drives for malware and suspicious items.
 - *Quick spyware scan* - scans your computer for installed (active) **spyware**. It does not scan all the folders and files on your computer, but only those that contain installed programs.
 - *Quick rootkit scan* - scans your computer for **rootkits** and other hidden and suspicious items.
 - *Perform full computer check* - scans the whole computer for viruses, spyware and rootkits.
3. The Scan Wizard guides you through the scanning and cleaning process. For more information, see “*Using The Scan Wizard*”, 44.

3.1.3 Quarantined Items

The Quarantine repository contains all **malware** (**viruses** and **spyware**), **riskware** and suspicious items that have been found and moved into the Quarantine repository. Quarantined items are isolated so that they do not pose any threat to your computer. For more information, see “*Quarantine*”, 30.

To open the Quarantine repository:

1. Go to the Virus and Spy Protection tab.
2. Click **Configure...** next to *Quarantined items*.

Viruses

The Quarantine repository *Virus* tab lists **viruses** that have been found and moved into the Quarantine repository. Quarantined items are isolated so that they do not pose any threat to your computer.

Spyware

The Quarantine repository *Spyware* tab lists all suspected spyware that has been found and moved into the Quarantine repository. You can restore quarantined spyware objects to your computer later. Quarantined items are isolated so that they do not pose any threat to your computer.



When Virus and Spy Protection detects a new spyware in your computer, you should quarantine it. You can delete the quarantined spyware after you have tested that all your applications still run correctly.

Riskware

The Quarantine repository *Riskware* tab lists all suspected riskware that has been found and moved into the Quarantine repository. You can restore quarantined **riskware** items to your computer later. Quarantined items are isolated so that they do not pose any threat to your computer.

3.2 Advanced Virus and Spy Protection

You can view the status and configure the following options with the advanced Virus and Spy Protection settings:

Selection	Description
Virus and Spy Protection	Displays the current Virus and Spy Protection level. Click Change... to change your Virus and Spy Protection level. For more information, see “ <i>Virus and Spy Protection Level</i> ”, 19.
Real-time Scanning	<i>Enable or disable</i> Real-time Scanning.
Scheduled Scanning	<i>Enable or disable</i> Scheduled Scanning.
System Control	<i>Enable or disable</i> System Control.



*You cannot change some Virus and Spy Protection settings if you use a High or Normal **protection level**. If you want to configure all settings manually, select Custom as your virus protection level.*

3.2.1 Real-time Scanning


On the Real-time Scanning page, you can select what to scan automatically in real time and what to do when a **virus**, **spyware** or other **malware** or suspicious item is found.



To enable real-time scanning, select the *Enable real-time scanning* check box.

When the real-time scanning is enabled, any file you open or close is automatically scanned for viruses, spyware and **riskware**.

Anti-Virus

Scanning Options

Scan all files	Scans all files for viruses. We recommend scanning all files, unless the computer is slow. You can speed up the system performance by scanning defined files only. There is a small risk of missing some infections when scanning defined files only.
Scan defined files	Scan only a predefined set of files. This option is recommended for the real-time protection. Click View... to define files that you want to scan.
	 <i>You cannot remove system defined file extensions but you can add more files to the scan. To specify files that have no extension, type '.' You can use the wildcard '?'.</i>
Scan inside compressed files	Scans files inside compressed ZIP, ARJ, LZH, RAR, CAB, TAR, BZ2, GZ, JAR and TGZ archives.

-  *Scanning inside large compressed files uses a lot of system resources and slows down the system. Therefore it is not recommended with the real-time protection. This setting is for advanced users only. Do not enable this setting unless you have a specific reason to do so.*
-  *You cannot change some Virus and Spy Protection settings if you use a High or Normal protection level. If you want to configure all settings manually, select **Custom** as your virus protection level.*

Actions

When virus is found	<p>Select what to do when a virus is found during the real-time scan. Choose one of the following actions:</p> <p><i>Ask what to do</i> - Opens the virus detection dialog when an infected file is found. For more information, see “Virus Detection”, 41.</p> <p><i>Disinfect automatically</i> - Disinfects viruses and deletes worms and trojans automatically when they are found.</p> <p><i>Rename automatically</i> - Renames the infected file automatically when a virus is found. Renamed infected file stays on your computer, but it cannot cause any damage.</p> <p><i>Delete automatically</i> - Deletes the infected file automatically when a virus is found.</p> <p><i>Report only</i> - Indicates that a virus is found, and does not let you open the infected object. This option only reports the virus, but does not take any action against it.</p>
---------------------	--



The action options are product specific.

Quarantine...

Opens the Quarantine repository. For more information, see “[Quarantined Items](#)”, 21 and “[Quarantine](#)”, 30.

Exclusions...

View and edit infected items and files, folders or file types that are not scanned. For more information, see “[Exclusions](#)”, 34.

Flyer History

Opens a list of logged System Control events. For more information, see “[Flyer History](#)”, 29.

Anti-Spyware

Scanning Options

Scan for spyware

Scans files for spyware during the real-time scanning. The scan detects suspicious applications when they are installed to your computer. If you disable the real-time spyware scan, you can still use the manual scanning to detect spyware. For more information, see “[Scanning Manually](#)”, 43.

Block tracking cookies

Removes detected **tracking cookies** automatically.

By default, you should leave this setting enabled. Disable the setting if a web site you want to view requires tracking cookies to work



*You cannot change some Virus and Spy Protection settings if you use a High or Normal protection level. If you want to configure all settings manually, select **Custom** as your virus protection level.*

Actions

When **spyware** is found

Ask what to do - Opens the spyware detection dialog when spyware is found. For more information, see “*Spyware Detection*”, 42.



The action options are product specific.

Show notification flyer for automatic actions

Displays a flyer on the bottom right-hand corner of your screen every time an automatic action is performed.

Quarantine...

Opens the Quarantine repository. For more information, see “*Quarantined Items*”, 21 and “*Quarantine*”, 30.

Exclusions...

View and edit spyware items and files, folders or file types that are not scanned. For more information, see “*Exclusions*”, 34.

Flyer History

Opens a list of logged System Control events. For more information, see “*Flyer History*”, 29.

System Control

Settings

Enable System Control

When enabled, System Control protects your computer from unwanted system modifications. If an application tries to perform a potentially dangerous action, it will be checked for trust. Safe applications are allowed to operate, while actions by unsafe applications are blocked.

Prevent all ActiveX from running

(For expert users only) Prevents your web browser from running ActiveX web applications. Some web sites may use ActiveX to install unwanted software on your computer. However, there are also web pages, which you cannot view without ActiveX. Allow ActiveX when you view this kind of web site.

ActiveX protection can be enabled only when System Control is enabled.



*You cannot change some Virus and Spy Protection settings if you use a High or Normal protection level. If you want to configure all settings manually, select **Custom** as your virus protection level.*

Action on system modification attempt

Ask my permission - System Control asks you whether you want to allow or block all monitored actions, even when System Control identifies the application as safe.

Ask when case is unclear - System Control asks you whether you want to allow or block monitored actions only when System Control cannot identify the application as safe or unsafe (default option).

Automatic: Do not ask - System Control blocks unsafe applications and allows safe applications automatically without asking you any questions.

Show notification flyer on deny events. Displays a flyer on the bottom right-hand corner of your screen every time an event is denied.

Applications Opens the System Control application dialog that lists all applications that have attempted to modify the system. For more information, see “*Applications*”, 35.

Flyer History Opens a list of logged System Control events. For more information, see “*Flyer History*”, 29.

Flyer History

Flyer History displays all logged System Control events.

System Control logs the following events:

- System start-up settings are changed.
- Application hijack is detected.
- Critical **file association** is changed.
- Critical system changes.

Click **Details...** to view more information about the event.

Click **Clear All** to clear the event list.

Quarantine

The Quarantine repository displays the following information about quarantined **viruses**, **spyware** and **riskware** items:

Virus

The *Virus* tab displays the following information.:

Name of malware	Displays the name of the quarantined virus. Click the name to connect to the Internet for more information.
Pathname	The path to the quarantined infected file.
Properties	Link to detailed information about the selected virus in the F-Secure online database.
Delete	Deletes the selected quarantined item from the Quarantine repository. You can delete items that you know you do not want to restore later.
Restore	Restores the selected item to your computer. Restored items are not excluded from subsequent scans so Virus and Spy Protection finds and notifies you about them.
Virus Details	
Name	The name of the quarantined malware. Click the name to connect to the Internet for more information.
File	The path and name of the quarantined file.
Size	The size of the malware in the Quarantine repository.
Date	The date and time when the malware was found during the scan and moved into the Quarantine repository.

Spyware

The *Spyware* tab displays the following information:

Name	Displays the name of the quarantined spyware object. Click the name to connect to the Internet for more information.
Type	Displays the quarantined spyware category: adware , data miner , dialer , malware , monitoring tool , riskware , vulnerability , worm or miscellaneous.
Included In	Displays the list of common applications that typically install the spyware.
Description	Displays a short description of the spyware type.

Properties

Displays detailed information of the selected spyware.

Delete

Deletes the selected spyware from the Quarantine repository.

You can delete applications that you know you do not want to restore later.

Restore

Restores the selected spyware to your computer. Restored items are not excluded from subsequent scans so Virus & Spy Protection finds and notifies you about them

Spyware Details

Name	The name of the quarantined spyware. Click the name to connect to the Internet for more information.
Type	The type of the quarantined spyware, such as data miner or monitoring tool .

TAC score	<p>Displays the Threat Assessment Chart (TAC) score. TAC score is not available for all spyware items.</p> <p>For more information, see the Threat Assessment Chart in: http://www.f-secure.com/spyware-info</p>
Size	<p>Displays the size of the spyware in the Quarantine repository.</p>
Date	<p>Displays the date and time when the spyware was found during the scan and moved into the Quarantine repository.</p>
Included In	<p>Applications in which this spyware is typically included.</p>
Description	<p>Short description of the spyware type.</p>

Riskware

Name of malware Displays the name of the quarantined riskware item. Click the name to connect to the Internet for more information.

Pathname The path to the quarantined riskware item.

Riskware Details

Name The name of the quarantined riskware item. Click the name to connect to the Internet for more information.

Type The type of the quarantined riskware item.

File The path and name of the quarantined riskware item.

Size Displays the size of the riskware in the Quarantine repository.

Date Displays the date and time when the riskware item was found during the scan and moved into the Quarantine repository.

Included In Applications in which this riskware item is typically included.

Description Short description of the riskware item.

Click **Close** to close the Quarantine repository.



If you restore the quarantined spyware item, it starts to work again and can spy your computer and display advertising pop-ups.

Exclusions

If scanning a certain file, folder or file type takes a long time and you know that the object is not infected, or you get **false alarms** during the scan, you can exclude items from the **virus** scan.

The software that installed the **spyware** to your computer may stop working if you remove the attached spyware **application**. If you want to use the software application that installed the spyware application to your computer, you may have to restore it from the Quarantine repository and exclude the spyware application from the spyware scan.



IMPORTANT: *Excluded items are not scanned. Make sure that they are not infected when you exclude them and remember that excluded items can become infected later. Excluding items reduces the level of your Virus and Spy Protection.*

You can exclude any of the following items:


Applications

Displays all spyware items that have been excluded from the scan. Virus and Spy Protection does not warn you when it detects any of the listed spyware item.

Click **Remove** to remove the selected spyware from the exclusion list.

If you want to delete the removed spyware from your computer, scan the computer again. For more information, see “[Removing Viruses and Spyware From Your Computer](#)”, 41.

To add a spyware item to the exclusion list, see “[Spyware Detection](#)”, 42 and “[Scanning Manually](#)”, 43.

Objects	<p>Click Add... to select the files or folders you want to exclude from scanning. Click Remove to remove the selected file or folder object from the list.</p> <p>If you want to add all listed objects to the scan without clearing the list, clear the <i>Exclude objects</i> check box.</p> <p> <i>When you exclude a folder from scanning, all subfolders are excluded, too.</i></p>
File Types	<p>To exclude a file type from the scan, enter its filename extension and click Add... Click Remove to remove the selected file type from the list. Separate each file type with a space, for example, AVI BMP GIF.</p> <p>If you want to add all listed file types to the scan without clearing the list of file types, clear the <i>Exclude files with these extensions</i> check box.</p>

Applications

The System Control Applications dialog shows a list of all applications that have attempted to modify the system and have been detected by System Control.

Application	The name of the application.
Permission	Displays the currently used ruleset for the application.

Type	Displays whether the rule was created manually or by the system.
Details...	Opens the Application Detail dialog. For more information, see “ Application Details ”, 36.
Remove	Removes the selected application from the list.

Application Details

The *Application Details* dialog shows the following information:

Application

File name	Displays the executable path and file name.
Version info	Displays the version number of the application.

Permission

Deny	Select <i>Deny</i> to deny all System Controlled monitored actions.
Allow	Select <i>Allow</i> to allow all System Controlled monitored actions.

3.2.2 Scheduled Scanning

You can set Virus and Spy Protection to scan your computer at specific times by selecting the *Enable scheduled scanning* check box.

To set the scanning schedule:

1. Under Scan performed, select how often you want Virus and Spy Protection to scan your computer:
 - a. *Daily* - scans every day at the scheduled time. The weekdays on the right are all selected and greyed out.
 - b. *Weekly* - scans every week at the scheduled weekday and time. You can select as many weekdays from the right as you like, and the scan is performed on each of the selected days.
 - c. *Monthly* - scans every month at the scheduled date and time. You can select up to three days of the month on which the scan is performed.
2. From the Start time drop-down list, select the time when you want the scan to start.
3. If you want to start the scan only when you are not using the computer, select the *After computer is not used for* option and select the idle time from the drop-down list.

Scanned Files

The scheduled scanning scans all files and archives, which are listed in the *Scan defined files* setting in the *Manual Scanning* settings. For more information, see “[Manual Scanning](#)”, 38.

The scheduled scanning disinfects viruses and deletes **worms** and **trojans** automatically when they are found.

3.2.3 Manual Scanning

On the *Manual Scanning* page, you can select what to scan and what to do when **malware** is found.

To start a manual scan:

1. Click the Virus and Spy Protection tab.
2. Click **Scan my computer...**

Virus and Spyware Scanning

Scan all files Scans all files for viruses.



Scanning all files can take a long time (many hours).

Scan defined files Scan only a predefined set of files. Click **Edit...** to define files that you want to scan.



You cannot remove system defined file extensions but you can add more files to the scan. To specify files that have no extension, type '.' You can use the wildcard '?'.

Scan inside compressed files Scans files inside compressed ZIP, ARJ, LZH, RAR, CAB, TAR, BZ2, GZ, JAR and TGZ archives.



Scanning inside large compressed files might use a lot of system resources and slow down the system.

Actions

When virus is found You can select what to do when a virus is found during the manual scan. Choose one of the following actions:

Ask what to do - Displays a list of infected files where you can select the action you want. For more information, see "*Using The Scan Wizard*", 44.

Disinfect automatically - Disinfects viruses and deletes worms and trojans automatically when they are found.

Quarantine automatically - Moves the infected file automatically to the Quarantine repository when a virus is found.

Rename automatically - Renames the infected file automatically when a virus is found.

Delete automatically - Deletes the infected file automatically when a virus is found.

Report only - Notifies you when a virus is found but does not take any action against it.

When spyware is found

You can select the action that takes place when a spyware application is found during the manual scan. Choose one of the following actions:

Ask what to do - Displays a list of spyware items where you can select the action you want.

Quarantine automatically - Move all found spyware automatically into the Quarantine repository.

Delete automatically - Deletes the found spyware automatically.

Report only - Notifies you when spyware is found but does not take any action against it.

Show suspicious items after a full computer check	Displays a list of suspicious items after the full computer check. Suspicious items are hidden from the normal file and process listings and they may be harmful to your system. For more information, see “ Suspicious Items ”, 51.
Quarantine...	Opens the Quarantine repository. For more information, see “ Quarantined Items ”, 21 and “ Quarantine ”, 30.
Exclusions...	View and edit spyware objects and files, folders or file types that are not scanned. For more information, see “ Exclusions ”, 34.



You can continue to use your computer as normal while the manual scan is running in the background.

3.3 Using Virus and Spy Protection

With Virus and Spy Protection enabled, your computer is protected against **malware**, **spyware**, **riskware** and suspicious items. When you access any file, it is automatically scanned. For more information, see “*Removing Viruses and Spyware From Your Computer*”, 41.

You can scan the computer manually if you suspect that your computer may contain malware or if you want to scan your computer for **rootkits**. For more information, see “*Scanning Manually*”, 43 and “*Using The Scan Wizard*”, 44.

3.3.1 Removing Viruses and Spyware From Your Computer

If **malware**, **spyware**, **riskware** or a suspicious item is found during the real-time scan and you do not want to process it automatically, Virus and Spy Protection displays a relevant detection dialog where you can select what to do.

Virus Detection

When Virus and Spy Protection finds a **virus**, **worm** or **trojan** during real-time scanning, it displays the *Virus Detection* dialog.

In the *Virus* detection dialog, you can either:

- *Disinfect* the file to remove the virus infection,
- *Delete* the infected file, worm or trojan completely,
- *Quarantine* the file, or
- *None* - do nothing.



Only viruses can be disinfected, worms and trojans can be deleted.

To open the virus information page in the Internet:

⇒ Click the name of the virus.

To view more information about the virus infection and the infected file:

⇒ Click **Details**.

Spyware Detection

When Virus and Spy Protection finds **spyware**, such as **adware**, **data miner**, **dialer**, **malware**, or **monitoring tool** during the real-time scanning, it displays the *Spyware Detection* dialog.

In the *Spyware Detection* dialog, you can either:

- *Delete* the application
- *Quarantine* the application
- *Exclude* the spyware from the future scans and keep it on your computer
- *None* - do nothing

To open the spyware description page in the Internet:

⇒ Click the name of the application.

Riskware Detection

When Virus and Spy Protection finds **riskware** during the real-time scanning, it displays the *Riskware Detected* dialog.

In the *Riskware Detected* dialog, you can either:

- *Delete* the application,
- *Quarantine* the application,
- *Exclude* the riskware from the future scans and keep it on your computer, or
- *None* - do nothing.

To open the riskware description page in the Internet:

⇒ Click the name of the application.

3.3.2 Scanning Manually

The real-time detection ensures the strongest protection against **viruses**, **spyware** and other **malware**, and suspicious items automatically. It is recommended, however, that you scan your computer manually in the following cases:

- *After the installation.*
It is highly recommended that once the installation is finished, you download the latest **virus and spyware definition databases** and perform the full computer check to ensure there are no viruses on your computer.
The product Start-up Wizard downloads latest virus and spyware definition databases and scans your computer automatically.
- *Real-time scan or Scheduled scan* has detected a virus.
After you have removed the virus, you should scan all hard disks to ensure that your computer is clean of the virus.
- You have reason to believe there is a virus or other malware on your computer but real-time scanning has not detected anything.
In this case, you should get the latest virus and spyware definition databases and scan all hard disks on your computer to find possible viruses and spyware. Also, you should check the latest

Security News for information on any new viruses that cannot be dealt with at the moment but require a future virus definition database update.

- You want to scan your computer for **rootkits**.
If you want to ensure there are no suspicious **hidden files**, **hidden processes**, **hidden applications** or **hidden drives** in your computer, scan the system manually for rootkits.
- You want to scan a shared network folder on another computer that has no local antivirus protection.
- You want to scan all files, including archives.

For information about manual scan settings, see “[Manual Scanning](#)”, 38.

For information how to start the manual scan, see “[Scan My Computer](#)”, 20.

3.3.3 Using The Scan Wizard

The Scan Wizard opens when you start the manual scan.

For information about manual scan settings, see “[Manual Scanning](#)”, 38.

For information how to start the manual scan, see “[Scan My Computer](#)”, 20.

Scan

The *Scan* page displays the scanning progress.

Scan	The selected scan type.
Target	The scanned target paths.
Scanned	The number of items that have been scanned.

Skipped	The number of items that have been skipped as they are excluded from the scan or locked by the operating system. For more information, see “ <i>Exclusions</i> ”, 34.
Viruses	The number of viruses found during the scan.
Spyware	The number of spyware items found during the scan.
Riskware items	The number of riskware items found during the scan.
Suspicious items	The number of suspicious items found during the scan.
Status	The scanning status and the currently scanned item.

Stopping the Scan

Click **Stop** to stop the current scan. Click **Show Report** to view the virus scanning report of the files that were scanned before the scan was stopped. If the scan is stopped and **malware** was found during the scan, you can either resume scanning or clean all found items.

It is recommended that you resume the scan to find all infected files. Select *Resume scanning* and click **Next** to continue the scan.

Finishing the Scan

When the scan is complete and no infected files were found during the scan, click **Show Report** to view the virus scanning report. Click **Finish** to close the Scan Wizard.

Select one of the following options if infected files were found during the scan:

- *Automatic cleaning* to disinfect **viruses** and delete **worms** and **trojans** automatically.
- *I want to decide item by item* to continue to the *Virus Cleaning* page.

Click **Next** to continue.

Virus Cleaning

The *Virus Cleaning* page displays a list of infected files.

File	Displays the file name of the infected file.
Infection	Displays the name of the virus. Click the name to connect to the F-Secure Security Information Center at http://www.f-secure.com/v-descs/ for more information about the virus.
Action to take	Displays the currently selected action for the infected file. <i>Delete</i> - Deletes the file completely. <i>Disinfect</i> - Disinfects the file to remove the virus infection. <i>Quarantine</i> - Quarantines the infected file so that it cannot be run automatically. <i>None</i> - Leaves the infected file on your computer. It is strongly recommended that you either delete, disinfect, quarantine, or rename the infected file instead of leaving it on your computer.



Note that only viruses can be disinfectd, worms and trojans can be only deleted.

If you want to change the current action, choose files from the list and select a new action by clicking the appropriate button.

Click **Next** to perform the selected action on every listed file.

After the virus cleaning is complete, click **Next** to continue.



IMPORTANT: If the Scan Wizard fails to disinfect or delete the file, you can delete it manually. For more information, see “*Removing Viruses And Spyware Manually*”, 53.

Virus Properties

To open the Virus Properties, right-click the infected file and select *Details*.

The *Virus Properties* dialog displays detailed information of the infected file.

Infection	Displays the name of the virus. Click the name to connect to the F-Secure Security Information Centre at http://www.f-secure.com/v-descs/ for more information about the virus.
Type	Displays the infection type. The infection can be either virus , worm or trojan .
Infected file	Displays the name of the infected file.
File path	Displays the path to the infected file. Click the path name to open the folder in the Windows Explorer.
Action	Displays what was done to remove the infection.
Result	Displays whether the action succeeded or not.
Reason	If the action failed, displays the reason why.

Click **Close** to close the detailed view.

Spyware Cleaning

The *Spyware Cleaning* page displays a list of applications Virus and Spy Protection found during the scan.

Name	Displays the name of the application. Click the name to connect to the F-Secure Security Information Center at http://www.f-secure.com/spyware-info/ for more information about spyware.
Type	Displays the application type. The type can be data miner , dialer , malware , monitoring tool , vulnerability , worm or miscellaneous.
Action to take	Displays the currently selected action: <i>Delete</i> - Delete the application from the computer. <i>Quarantine</i> - Quarantine the application. For more information, see " <i>Quarantined Items</i> ", 21. <i>Exclude</i> - Exclude the application from the scanning. <i>None</i> - Leaves the application in your computer but does not exclude it from the scan.

If you want to change the current action, choose items from the list and select a new action by clicking the appropriate button.

Click **Next** to perform the selected action on every listed item.

After the spyware cleaning is complete, click **Next** to continue.

Spyware Properties

To open the Spyware Properties, right-click the application and select *Details*.

The *Spyware Properties* dialog displays the following information:

Name	Displays the name of the application. Click the name to connect to the F-Secure Security Information Center at http://www.f-secure.com/spyware-info/ for more information about spyware.
Type	Displays the quarantined application type. The application can be data miner , dialer , malware , monitoring tool , vulnerability , worm , or a miscellaneous application.
Description	Displays a short description of the spyware type.
Included in	Displays a list of applications that typically install the spyware.
Infected file:	Displays the name of the spyware.
File path:	Displays the path to the spyware item. Click the path to open it in the Windows Explorer.
Action	Displays the action that was taken on the detected application.
Result	Displays whether the action succeeded or not.
Reason	If the action failed, displays the reason why.

Click **Close** to close the detailed view.

Riskware Items

The *Riskware Items* page displays a list of riskware items Virus and Spy Protection found during the scan.

Name	Displays the name of the application. Click the name to connect to the Internet for more information.
Action to take	<p>Displays the currently selected action:</p> <p><i>Delete</i> - Delete the riskware item from the computer.</p> <p><i>Quarantine</i> - Quarantine the riskware item. For more information, see “Quarantined Items”, 21.</p> <p><i>Exclude</i> - Exclude the riskware item from the scanning.</p> <p><i>None</i> - Leaves the riskware item in your computer but does not exclude it from the scan.</p>

If you want to change the current action, choose items from the list and select a new action by clicking the appropriate button.

Click **Next** to perform the selected action on every listed item.

After the riskware item cleaning is complete, click **Next** to continue.

Riskware Properties

To open the Riskware Properties, right-click the **riskware** item and select *Details*.

The *Riskware Properties* dialog displays the following information:

Name	Displays the name of the application. Click the name to connect to the Internet for more information.
Type	Displays the quarantined riskware item.
Description	Displays a short description of the riskware item.

Included in	Displays a list of applications that typically install the riskware item.
Infected file:	Displays the name of the riskware item.
File path:	Displays the path to the riskware item. Click the path to open it in the Windows Explorer.
Action	Displays what was done to the detected riskware item.
Result	Displays whether the action succeeded or not.
Reason	If the action failed, displays the reason why.

Click **Close** to close the detailed view.

Suspicious Items

The *Suspicious Items* page displays a list of items that are hidden from normal file and process listings.

Item Name	Displays the name of the file, process or application.
Type	Displays the type of the item. The item type can be hidden file , hidden process , hidden application or hidden drive .
Action to take	Displays the currently selected action: <i>Automatic</i> - Let Virus and Spy Protection handle the item automatically.

Rename - Rename the item. Renamed items stay on your computer, but they cannot cause any damage.

Exclude - Exclude the item from the scan. Excluded items stay on your computer and are not displayed during subsequent scans.

None - Leaves the item in your computer but does not exclude it from the scan.

Suspicious Items Properties

To open Suspicious Items Properties, right-click the item and select *Details*.

The *Suspicious Items Properties* dialog displays the following information:

Suspicious item	Displays the name of the file, process or application.
File path	Displays the path to the suspicious file. Click the path to open it in the Windows Explorer.
Type	Displays the type of the item. The item type can be hidden file , hidden process , hidden application or hidden drive .
Description	Displays a short description why the item is suspicious.
Action	Displays what was done to the suspicious item.
Result	Displays whether the action succeeded or not.
Reason	If the action failed, displays the reason why.

Finish And Scan Report

When the scan is finished after malware was found, the *Finish* page indicates that the scan was finished. It displays if there were items that were not cleaned.

When the scan is complete, click **Show Report** to view the virus scanning report. If your computer is clean and no infected files were found during the scan, click **Finish** to close the wizard.

Scanning Report

When the scan is complete, Click **Scan Report** to view the report of the last scan.

The virus scan report contains details of every processed file and the action taken. Click the **malware** name to connect to the Internet for more information about the infection.

3.3.4 Removing Viruses And Spyware Manually

If the Scan Wizard fails to disinfect or delete the file it could be due to one of the following reasons:

- The **virus and spyware definition databases** are outdated. Make sure you have latest virus and spyware definition databases and retry. For more information, see “*Automatic Updates*”, 59.
- Manual disinfection is required.

In some cases, you need to run a tool that disinfects the file and removes the virus. Some viruses use advanced techniques to hide and attach themselves to your files and can be disinfecting only with a special tool. For more information, see [“How to Remove the Virus Manually”](#), 55.

- The infected file is read-only or you do not have permission to access the file.

The Scan Wizard can disinfect and delete only files that you have permission to access and change. If the Scan Wizard does not have the access to the file, start the computer in safe mode and log on with an account that has administrative rights and run the scan again.

- File is on a CD or inside an archive.

You cannot disinfect or delete files on CD or inside archives.

- False alarm.

Every care is taken to ensure that the product does not suspect a harmless file to be infected, but due to the complex nature of files, it may suspect a safe file.

- The **heuristic** scanner has discovered a new virus.

A new type of virus may have infected your computer. Don't panic. Your files are currently safe as the virus was detected and stopped before it caused any damage. For more information, see [“What if You Suspect You Have Found a New Malware?”](#), 55.



*Only viruses can be disinfecting, **worms** and **trojans** can be only deleted.*

If you are certain that the file is safe, you can ignore the warnings and you can set Virus and Spy Protection to ignore the file in the future. For more information, see [“Exclusions”](#), 34.

How to Remove the Virus Manually

If the Scan Wizard fails to disinfect or delete the file, follow these instructions to remove the virus by yourself:

1. Make sure you have the latest **virus and spyware definition databases**. For more information, see “*Automatic Updates*”, 59.
2. Check the F-Secure Computer Security Information Center at <http://www.f-secure.com/v-descs/> for information on the virus. The virus information can help you to remove the virus and may include a link to the tool necessary to remove the virus.

Removal tools contain all the necessary instructions for you to follow in order to remove the virus from your system.

3. If you have scanned your computer with the latest virus definition database without success and you have not been able to successfully use any disinfection tools from the F-Secure Security Information Center, see “*What if You Suspect You Have Found a New Malware?*”, 55.

3.3.5 What if You Suspect You Have Found a New Malware?

You may have a brand new **malware** on your computer if the product warns you that you have an infected file, but the Scan Wizard cannot disinfect or delete it.

Until you know that the possible **virus, worm or trojan** has been removed, or that it was a false alarm, you should not attempt to use the file.

To remove the malware, follow these steps:

1. Make sure you have the latest **virus and spyware definition databases** and scan your computer again. A new database may contain information on how to deal with the malware in your computer. For more information, see “*Automatic Updates*”, 59.
2. If you have scanned your computer with the latest virus and spyware definition databases, check the F-Secure Computer Virus Info Center at <http://www.f-secure.com/v-descs/> for information on the virus. The virus information can help you to remove the virus and may include a link to the tool necessary to remove the virus.
3. If the previous steps fail, send the infected file to F-Secure VirusLab. For instructions, go to:
<http://www.f-secure.com/support/technical/general/samples.shtml>.

3.3.6 Using System Control

F-Secure System Control is a new, host-based intrusion prevention system that analyzes the behavior of files and programs. It provides an extra-layer of protection by blocking undiscovered viruses, worms, and other malicious code that try to perform harmful actions on your computer.

Action on System Modification Attempt

In System Control, you can choose one of the three action modes:

- System Control asks you whether you want to allow or block all monitored actions, even when System Control identifies the application as safe.
- System Control asks you whether you want to allow or block monitored actions only when System Control cannot identify the application as safe or unsafe (default option).
- System Control blocks unsafe applications and allows safe applications automatically without asking you any questions.

For more information, see “*What To Do With System Control Pop-Ups*”, 57.

What To Do With System Control Pop-Ups

System Control detects an application trying to perform an action. If you know that it is safe to allow the application to perform the action, select *Allow, I trust the application* and click **OK**.

Applications that cannot be considered safe are:

- Applications you have not actively installed yourself, or have no knowledge of.
- Applications that you consider safe but which try to open the Internet connection without you starting them.
- A connection that displays IP address instead of **DNS** name as a target.
- Applications which try to start another applications or manipulate another running applications without you starting them.



*If you want to send a sample of an application that tried to modify the system, click the **Send a sample to F-Secure** link.*



4

AUTOMATIC UPDATES

Basic Automatic Updates	60
Advanced Automatic Updates	62

4.1 Basic Automatic Updates

The Automatic Update Agent activates transparently in the background any time you connect to the Internet so that you can receive the latest updates to your computer transparently.

Selection	Description
Automatic Updates	Shows the Automatic Updates status. Click Enable to activate or Disable to deactivate Automatic Updates.
Last update check	Shows the time and status of the latest update.
Next update check	Shows the time of the next update. If you want to check that you have the latest updates, click Check Now . If they are not up to date, the newest versions will be downloaded.
Virus definitions updated	Shows the time of the latest virus definitions update.
Spyware definitions updated	Shows the time of the latest spyware definitions update.
System Control	Shows the latest date when the System Control was updated.
Advanced...	Takes you to the Automatic Updates page of the <i>Advanced Settings</i> window. For more information, see “ <i>Advanced Automatic Updates</i> ”, 62.



If you are using a modem, or have an ISDN connection to the Internet, the connection must be active in order to check for updates



ISDN users: By default, Automatic Updates are scheduled once per hour. This means that an Internet connection will be opened once every hour if you have an ISDN router or similar auto-dialer (and each connection will cost you money). If you want to prevent your ISDN router from auto-dialing, disable Automatic Updates and click Check now to check for updates.

4.2 Advanced Automatic Updates

On the Automatic Updates page of the advanced settings, you can specify whether you want to automatically receive virus definition updates.

Selection	Description
Status	
Automatic Updates	Shows the Automatic Updates status. Click Enable or Disable to change the current status.
Details	
F-Secure Update Server	Shows the address where the product downloads new updates.
Last update check	Shows the time and status of the latest update.
Next update check	Shows the time of the next update. If you want to manually check that you have the latest updates, click Check Now . If they are not up to date, the newest versions will be downloaded.
Updates	
Virus definitions	Shows the date and the version number of currently used virus definitions.
Spyware definitions	Shows the date and the version number of currently used spyware definitions.
System Control	Shows the latest date when the System Control was updated.

4.2.1 Connection

To define how you are connected to the Internet, change Internet Connection settings. For more information, see “[Internet Connection](#)”, 63.

To see a reminder when virus definitions are older than the specified number of days, select the *Show reminder when virus definitions are older than x days* check box.

Internet Connection

There are three options for identifying whether an Internet connection is available:

1. *Assume always connected* - Automatic Updates always assumes that there is an active network connection. Note that if the computer does not actually have a permanent network connection and is set up for dial-on-demand, this behavior can result in multiple dial-ups initiated by the Automatic Updates.
2. *Detect connection* - Automatic Updates attempts to detect whether the network connection is active, and tries to communicate only when there appears to be a network connection. This is the default setting.
3. *Detect traffic* - Automatic Updates attempts to detect whether the network connection is active by detecting if other applications are using the network. Recommended for computers without a permanent connection to the network, but with unusual hardware configurations that cause "Detect connection" to decide that there is always a network connection.

4.2.2 HTTP Proxy

On the HTTP Proxy page, you can set up your proxy settings for Automatic Updating using Proxy. You can select either:

- *No HTTP proxy* if you want to use a direct connection.
- *Manually configure HTTP proxy* if you want to configure proxy settings specifically for Proxy. Click **Configure...** to open the *HTTP Proxy Setup* dialog.
- *Use my browser's HTTP proxy* if you want to use the same proxy settings already set up in your default browser.

HTTP Proxy Setup

In the *HTTP Proxy Setup* dialog, enter the settings of your proxy server. First, enter the address and port number of the proxy server in the *Address* and *Port* fields.

- If you want the update to stay in the proxy cache after you have downloaded it, select the *Allow proxy to cache updates* check box. This allows other users to download the update directly from the proxy without the proxy having to download it from the update server again.
- If the proxy server requires user authentication, select the *Proxy requires user authentication* check box and enter your user name and password in the *User name* and *Password* fields.

4.2.3 Downloads

The *Downloads* list displays all downloaded software packages, when they have been received and whether they have been installed or not.

- Click **Show Log File...** to view the log that displays the download information.
- Click **Details...** to view additional information on the selected software package.
- Click **Install** to install the selected software package, if it has not been installed already.

GLOSSARY

ActiveX

ActiveX is a set of technologies from Microsoft that enables interactive content for the World Wide Web. As ActiveX security settings in Internet Explorer can allow web pages to secretly install ActiveX controls automatically, they can be a significant security threat. ActiveX controls can access files on your hard drive.

adware

Adware, short for advertisement software, is a software program that displays advertising material in your web browser. Some adware programs collect information about your browsing habits and computer use. Based on that information, they automatically download advertising material on your computer and display it. Some adware programs are installed together with other software programs. These other software programs may stop functioning if adware is removed.

application

Application is a software program designed for a specific purpose. For example, word processors, spreadsheets and media players are all applications. Malicious applications are known as malware.

browser hijacking

An application which attempts to take control of your web start page, or other web sites you are likely to visit, is known as browser hijacker. Browser hijacker tries to force you to visit a web site to inflate the traffic for higher advertising revenues.

data miner

A data miner is a program that can collect information how you browse and use web sites, including data gathered from forms you fill and submit to different web sites. Usually data miners work without your knowledge.

Denial-of-Service (DoS) attack

An explicit attempt by attackers to prevent legitimate users of a service from using that service by disrupting connections, "flooding" a network or preventing a particular individual from accessing the network.

dialer

A dialer is a program which tries to connect to expensive pay-per-minute phone number using the modem. Most dialers work without your awareness or permission.

DNS

The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember name for an Internet address. The Internet address `www.example.com` is an example of a DNS name.

file association

A file association is an association between a file and a program that can use those files. For example, the program that opens an image file when you double-click it is based on file associations. When you install new software on your computer, it may set up associations to files, which were associated with other programs.

false alarm

You can get a false virus alarm when the product detects a virus in an uninfected file. Every care is taken to ensure that the product does not suspect a harmless file to be infected, but due to the complex nature of files, it may suspect a safe file.

heuristic

Exploratory problem-solving that utilizes self-educating techniques.

hidden application

Hidden applications are not visible, the application process and the file are both hidden from users. It is possible that a rootkit is hiding the application from Windows Task Manager.

hidden drive

Hidden drives are not visible to users.

hidden file

Hidden files are not visible to users. It is possible that a rootkit is hiding the file from the normal file listings.

hidden process

Hidden processes are not visible to users. It is possible that a rootkit is hiding the process from Windows Task Manager.

hosts file

The Hosts file is a lot like an address book. When you type an address into your web browser, the address is translated into a numeric IP address. If this translation information can be found from the Hosts file your computer will use it, otherwise it will connect to the DNS service of your Internet Service Provider.

Some malware can edit your Hosts file to hijack and redirect any connection to a web page to some other page in the Internet.

keylogger

A keylogger is a program that monitors each keystroke you type on the keyboard. This information may include for example your passwords and credit card numbers.

A keylogger can be installed to your computer as a part of spyware or trojan.

malformed message

Unsolicited bulk e-mails may contain poorly or intentionally malformed e-mail headers to disguise their origin, which makes tracing them more difficult.

malware

Malware, short for malicious software, is any program that is designed specifically to damage or disrupt your computer. Examples of malware are viruses, worms, and trojans. Malware can take control over your web browser, redirect your search attempts, show pop-up ads, keep track on the web sites you visit, and steal personal information like your banking information. Malware programs can also cause your computer to become slow and unstable.

monitoring tool

A monitoring tool can monitor and record all computer activities, including each keystroke you type on the keyboard.

packet

A packet is the unit of data that is routed between an origin and a destination on the Internet. When any file (e.g. an e-mail message) is sent from one place to another on the Internet, the file is divided into packets of an efficient size for routing. When they have all arrived, they are reassembled into the original file at the receiving end.

phishing

Phishing (pronounced fishing) is a scam technique that is used to steal personal information. It uses false e-mail messages that appear to come from legitimate businesses and link to false, but genuine-looking web sites. These authentic-looking messages are designed to fool people into giving away personal data, such as bank account numbers, passwords, and credit card and social security numbers.

protection level

Protection levels are preconfigured attributes that set your level of security. They are automatically updated so that you are protected against the latest forms of malicious computer programs and Internet attacks.

quarantine

Quarantined items are isolated so that they do not pose any threat to your computer.

The Quarantine repository contains all applications that have been detected during the scan and moved into the Quarantine repository. You can add new applications to the Quarantine when Virus & Spy Protection detects them.

recursive archive

Recursive archive files, also known as nested archives, are archives that contain other archives inside.

riskware

Riskware is any program that does not intentionally cause harm but can be dangerous if misused, especially if set up incorrectly. Examples of such programs are programs for chatting (IRC), or programs for transferring files over the Internet from one computer to another. If you have explicitly installed this program, it is less likely to be harmful. If riskware is installed without your knowledge, it is most likely installed with a malicious intent and should be removed. The difference between riskware and malware is that malware is specifically designed to damage your computer.

rootkit

Rootkits are typically used to hide malicious software from users, system tools and antivirus scanners. Not all rootkits are malicious by themselves but they are often used to hide viruses, worms, trojans and spyware.

spam

Spam messages are mass mailed e-mail copies of the same message which are sent to people who would not otherwise choose to receive them.

spyware

Spyware is a legal software that you may not want. It almost always installs itself without your permission, for example, as the result of clicking an option in a misleading pop-up window, or together with a useful program. Some spyware programs collect information on your browsing habits for a third party, which can be a person, a server, or another software program. Some spyware programs can also gather information about your e-mail addresses, passwords and credit card numbers.

subnet

Short for "subnetwork", it is a section of a network. Usually, computers within the same subnet will be physically near to each other and will have IP addresses that begin with the same two or three numbers.

TAC score

The TAC score determines how likely the application is malware, 1 being the least and 10 being the most problematic. The product does not notify you about objects with TAC score of 2 or less.

tracking cookie

Tracking cookies track your web browsing habits. They can collect information of pages and advertisements you have seen or any other activity during the browsing. Different websites can share tracking cookies and each website with the same tracking cookie can read and write new information into it.

trojan

A trojan is usually a standalone program that performs destructive or other malicious actions. Destructive actions can vary from erasing or modifying the contents of files on a hard drive to a complete destruction of data.

A backdoor trojan is a remote access tool that can allow a hacker to get full control over the entire infected system. They can send, receive and run files and even listen and see what happens at the computer if it is equipped with a microphone or a webcam.

virus

A virus is usually a program that can attach itself to files and replicate itself repeatedly. Viruses can alter and replace the contents of other files.

virus and spyware definition databases

Virus definition databases and spyware definition databases are used to detect viruses and spyware. You need to keep databases updated so that Virus & Spy Protection can detect latest viruses and spyware.

vulnerability

Vulnerabilities open security holes that can allow other applications to connect to the system without your authorization or knowledge.

worm

A worm is a program that can replicate itself by sending copies in e-mail messages or over a network.

Internet worms are also known as mass-mailers. Mass-mailers usually send themselves as e-mail attachments to e-mail addresses that they can find on the infected computer. In some cases, an infected attachment can start automatically, in other cases the user has to open the attachment to become infected.

F-SECURE®



www.f-secure.com