

# **F-Secure Internet Security 2003**

**Win 95/98/ME/NT4.0/2000/XP**

**User's Guide**

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.

Copyright © 1996-2003 F-Secure Corporation. All rights reserved.

# Contents

<b>About This Guide .....</b>	<b>1</b>
Glossary of Icons .....	2
<b>1. Installing F-Secure Internet Security 2003 .....</b>	<b>3</b>
1.1 Before You Begin .....	3
1.2 Installation Steps .....	4
1.3 If you Need to Uninstall F-Secure Internet Security 2003 .....	6
<b>2. Getting Started .....</b>	<b>9</b>
2.1 Using F-Secure Internet Security 2003 for the First Time .....	9
2.2 What to do When the Application Control Pop-Up Appears .....	9
2.3 Is F-Secure Internet Security 2003 Active and Working Properly? .....	11
2.4 Options for Accessing F-Secure Internet Security 2003 .....	13
<b>3. Home .....</b>	<b>19</b>
<b>4. Virus Protection .....</b>	<b>21</b>
4.1 Virus Protection Profiles .....	22
4.2 Scan for Viruses .....	23
4.3 Removing a Virus from your Computer .....	25
4.4 What if you Suspect you Have Found a New Virus? .....	33
4.5 Setting Protection to Ignore/Scan Selected Files .....	34
<b>5. Internet Shield .....</b>	<b>37</b>
5.1 Internet Shield Profiles .....	38
5.2 Using Application Control .....	39
5.3 Customizing Internet Shield Rules .....	43

5.4 Advanced Settings .....	52
<b>6. Automatic Updates .....</b>	<b>55</b>
<b>7. My Subscription .....</b>	<b>59</b>
<b>8. How F-Secure Internet Security 2003 Protects Your Computer .....</b>	<b>61</b>
8.1 Viruses Protection .....	61
8.2 Internet Shield .....	62
8.3 How Can You Help to Avoid Viruses and Other Malware .....	63
<b>Troubleshooting .....</b>	<b>65</b>
Installation .....	65
General Use .....	65
Virus Protection .....	66
Internet Shield .....	67
Automatic Updates .....	68
<b>Glossary .....</b>	<b>69</b>
<b>Support and Maintenance .....</b>	<b>73</b>
Technical Support .....	74
Maintenance .....	75

## About This Guide

This guide provides all the information you need to install and use F-Secure Internet Security 2003.

**Chapter 1.** *Installing F-Secure Internet Security 2003.* Provides the necessary information for you to install F-Secure Internet Security 2003.

**Chapter 2.** *Getting Started.* Offers information for new users and a reference for more experienced users on how to access and get started using F-Secure Internet Security 2003.

**Chapter 3.** *Home.* Offers you a quick and detailed overview of your security settings and F-Secure Internet Security 2003's status.

**Chapter 4.** *Virus Protection.* Explains how you can enable or disable virus protection, select your virus protection profile and monitor when you have received virus definition updates.

**Chapter 5.** *Internet Shield.* Explains how you can change and edit Internet Shield profiles, see how many connections have been allowed or denied, and access advanced settings.

**Chapter 6.** *Automatic Updates.* Offers information on the automatic update service that provides you with the latest virus information, software versions and profile versions.

**Chapter 7.** *My Subscription.* Explains how you can view your subscription status, renew your subscription and change your subscription number.

**Chapter 8.** *How F-Secure Internet Security 2003 Protects Your Computer.* Defines the threats against your computer and explains how F-Secure Internet Security 2003 protects your computer against these threats.







*Troubleshooting* - solves some common problems.

*Glossary* - explanation of terms.

[Support and Maintenance](#) - contains the contact information for assistance.

## Glossary of Icons

The following icons appear in F-Secure Internet Security 2003:

	Enabled	The feature is enabled and working properly.
	Question	A question that may require you to make a decision.
	Info	Informative text to help you use F-Secure Internet Security 2003.
	Busy	Please wait.
	Warning	An F-Secure Internet Security 2003 feature is disabled or your virus definitions have not been updated recently.
	Error	An error has occurred. Please read the error message carefully.

**Note:** Some icon meanings differ on the My Subscription page. For more information, see [Chapter 7. My Subscription](#). on page page 59.

# 1. Installing F-Secure Internet Security 2003

## 1.1 Before You Begin

### *System Requirements*

Your computer must meet the following requirements to install and run F-Secure Internet Security 2003:

Processor:	Intel Pentium II or higher
Operating System:	Microsoft® Windows® 95/98/ME/NT4.0 (SP6 required)/2000/XP
Memory:	Windows 95/98/ME/NT4.0 - 64 MB of RAM Windows 2000/XP - 128MB of RAM
Disk Space:	30 MB free hard disk space (60 MB during installation)
Display:	Minimum 256 colors
Internet Connection:	An Internet connection is required in order to validate your subscription and receive updates
Browser:	Internet Explorer 3.0 or newer is required

## **Preparing your Computer for Installation**

Running several different antivirus and firewall programs at the same time is not recommended. Conflicting antivirus software can corrupt and damage your files.

### ***Removing Other Antivirus/Firewall Software***

F-Secure Internet Security 2003 can automatically upgrade versions of F-Secure Anti-Virus 4 and 5, and F-Secure Distributed Firewall 5.

Antivirus and firewall programs from other vendors must be uninstalled separately before you install F-Secure Internet Security 2003. Please refer to the appropriate vendor's documentation to uninstall the software.

## **1.2 Installation Steps**

---

**Note:** If you are using Windows NT 4.0, Windows 2000 or Windows XP and have more than one account, you have to log in as an administrator to install F-Secure Internet Security 2003.

---

To install F-Secure Internet Security 2003, please follow these instructions:

### ***Part 1: Installing F-Secure Internet Security 2003***

1. Close all other programs, and insert your F-Secure Internet Security 2003 CD into the CD-Rom drive on your computer.



Installation should now start automatically. If it does not start, browse the CD and open the Setup directory. Locate the file *install.exe* and double-click it to start the installation.

2. Choose the language you want to use for this installation and click **Next** to continue.
3. Read the subscription agreement and if you agree to the terms, click your mouse on the *I accept the agreement* checkbox. Click **Next** to continue.
4. Choose the directory to which you want to install F-Secure Internet Security 2003. Click **Next** to continue.
5. Files are transferred to your computer. When the transfer is complete, continue to the second part of the installation.

---



**Note:** You may be asked to restart your computer. Select *Restart Now* (If you select *Restart Later*, installation will not continue until the computer is restarted) and click **Finish** to continue.

---

### ***Part 2: Selecting Components and Validating Your Subscription***

1. To validate your subscription, ensure that your Internet connection is active. You are prompted to either:
  - Enter your subscription number to register your subscription. Click **Next** to continue.
  - Select to evaluate the product (if you are installing in evaluation mode). Click **Next** to continue. Choose your preferred type of installation from the following window, and click **Next** to continue.

---

**Tip:** You can follow the installation progress by double-clicking  in the Windows system tray at the bottom right of your screen. This icon will be replaced with the  icon when the installation is complete.

---

2. After F-Secure Internet Security 2003 has installed the necessary files, you are asked to restart your computer. Select *Restart Now* (If you select *Restart Later*, installation will not be complete until the computer is restarted). Click **OK** to finish the installation.

To make sure the installation was successful, see [“Is F-Secure Internet Security 2003 Active and Working Properly?”](#) on page 11.

---

**Note:** After installation is complete, Application Control may prompt you to allow or deny any application that tries to connect to the Internet. For instructions, see [“What to do When the Application Control Pop-Up Appears”](#) on page 9.

---

### 1.3 If you Need to Uninstall F-Secure Internet Security 2003

Uninstall F-Secure Internet Security 2003 using the Windows *Add/Remove Programs* feature found in the Windows control panel. This will ensure safe and complete removal of the program from your computer. To do this:

1. Open the Start menu in your Windows taskbar.
2. Select *Settings -> Control Panel -> Add/Remove Programs*.

3. Select *F-Secure Internet Security 2003* and click **Remove**.
4. Restart your computer.



## **2. Getting Started**

### **2.1 Using F-Secure Internet Security 2003 for the First Time**

If you are running F-Secure Internet Security 2003 for the first time, see the following sections to assist you in ensuring that F-Secure Internet Security 2003 is running, and protecting you according to your security needs.

- What to do When the Application Control Pop-Up Appears.
- Is F-Secure Internet Security 2003 Active and Working Properly?
- Options for Accessing F-Secure Internet Security 2003.

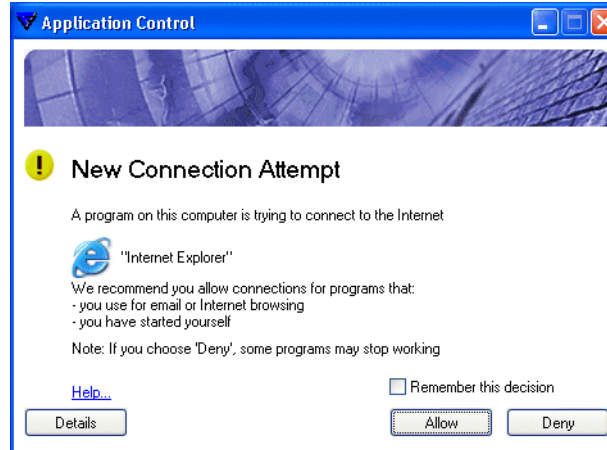
### **2.2 What to do When the Application Control Pop-Up Appears**

When F-Secure Internet Security 2003 is installed, Application Control may prompt you when an application attempts to connect to the Internet, depending on your Internet Shield profile.

Application Control allows for safe browsing and is an excellent defence against malicious computer programs such as Trojans (for a definition of a Trojan horse and other terms, see the *Glossary* on page 69). It will, however, cause a number of requests to deny or allow connections to a particular address in the beginning. The number of requests will decrease and you will rarely see Application Control pop-ups, unless you install new software or if a malicious application attempts to connect to the Internet from your computer.

**Example: Starting Your Internet Browser for the First Time After Installation**

1. Start your Internet browser (e.g. Internet Explorer, Netscape).



2. The Application Control pop-up appears, asking you whether the *Internet Explorer* connection attempt should be allowed or denied.
  - a. Select *Remember this decision in the future* as you know that your Internet browser is a safe application.

- b. Click **Allow** as you know that the browser you are starting yourself is safe (to learn more about what can be considered safe or unsafe, see “*Using Application Control*” on page 39).

You can click **Help** to learn more about Application Control.


---

**Note:** If you want to turn off the Application Control feature, go to the Internet Shield page. Beside Application Control, click **Change**. The status text will change from *Prompt* to *Allow and log*.

---

For more information on Application Control, see “*Using Application Control*” on page 39.

## 2.3 Is F-Secure Internet Security 2003 Active and Working Properly?








After you have installed, or anytime you are using F-Secure Internet Security 2003, you can check that F-Secure Internet Security 2003 is active and working properly from the  icon in your Windows system tray at the bottom right corner of your screen as shown below:





**Note:** In Windows XP, icons may be hidden. To show the hidden icons, click the  button.

---

The icon may appear differently or not at all depending on the status of F-Secure Internet Security 2003. See the list of icons and their meanings in the table below:

Icon	Meaning	What To Do
	F-Secure F-Secure Internet Security 2003 is working properly. Your computer is protected.	Use your email and browse the Internet as normal.
	Installation in progress. Your computer is not yet protected.	Wait for installation to finish. The  icon will appear when installation is complete.
	Error state. An error has occurred in F-Secure Internet Security 2003.	Place your mouse pointer over the  icon to see the reason for the error. If necessary, restart your computer.
	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 tool-tip. Enable the feature that is currently disabled or go to F-Secure Internet Security 2003 and check for updates.



Icon	Meaning	What To Do
	Unloaded. F-Secure Internet Security 2003 is deactivated and your computer is not protected.	Right-click the  icon and select <i>Reload</i> to activate F-Secure Internet Security 2003.
No icon	F-Secure Internet Security 2003 is not installed. Your computer is not protected.	Restart you computer and install F-Secure Internet Security 2003.

## 2.4 Options for Accessing F-Secure Internet Security 2003

There are several ways of accessing and using F-Secure Internet Security 2003:

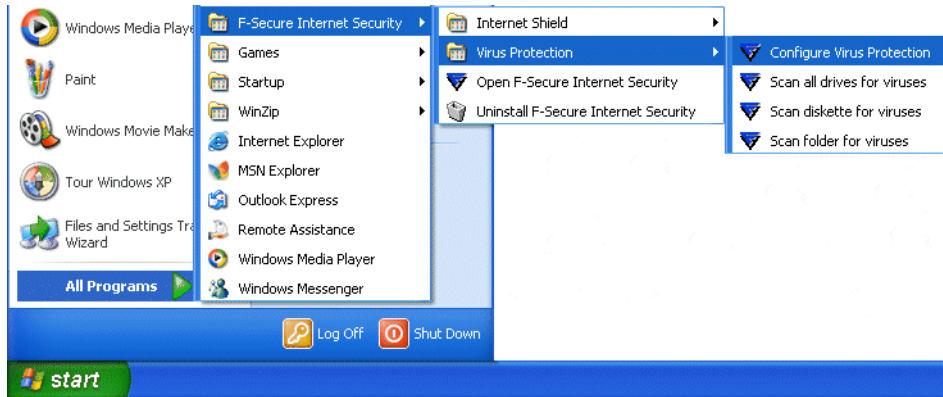
- Windows Start Menu
- The F-Secure Icon
- F-Secure Internet Security 2003 Windows Explorer Pop-Up Menu

### Windows Start Menu

To open F-Secure Internet Security 2003, access basic operations, view manuals and web pages:


1. Open the Windows *Start* menu.

2. Go to the *Programs* menu and the F-Secure Internet Security 2003 sub-menu.
3. Click Open F-Secure Internet Security 2003 to start using F-Secure Internet Security 2003, or select another option from the F-Secure Internet Security 2003 sub-menu.



## The F-Secure Icon

You can use the F-Secure icon (  ) in the Windows system tray (at the bottom right corner of your screen) to open F-Secure Internet Security 2003, view the status of F-Secure Internet Security 2003 or access the F-Secure Internet Security 2003 pop-up menu.

To open F-Secure Internet Security 2003, double-click the  icon with your left mouse button.

### ***F-Secure Internet Security 2003 Status Tool-Tip***

Place your mouse over the icon to show the F-Secure Internet Security 2003 status tool-tip. With the tool-tip, you can instantly see if F-Secure Internet Security 2003 has a problem, as shown in the example below where Virus Protection has been disabled.



### ***F-Secure Internet Security 2003 Pop-Up Menu***

Click the icon with the right mouse button to access the F-Secure Internet Security 2003 pop-up menu with its list of common and frequently used operations. From the menu, you can open F-Secure Internet Security 2003 or instantly scan for viruses.



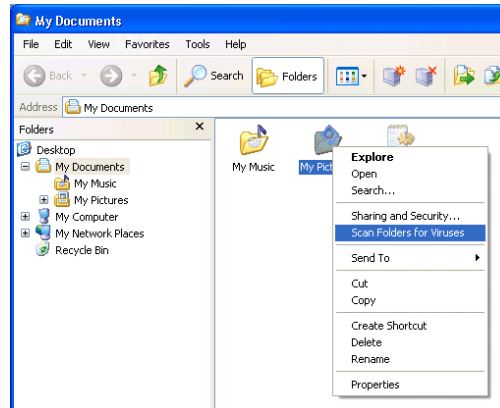
To get a better understanding of each of the menu items, see the table below:

<b>Selection</b>	<b>Explanation</b>
Open F-Secure Internet Security 2003	Opens F-Secure Internet Security 2003.
Unload F-Secure products	Unload products from memory. Sometimes this is necessary when installing some software, or doing performance-critical tasks. Do not leave you computer in this state for extended periods, as it is not protected.
Scan All Hard Disks	Virus Protection scans all available hard disks on your computer.
Scan Diskette	Virus Protection scans any floppy disk in the A: drive.
Scan Target...	Virus Protection scans the target of your choice. A directory tree appears. Select your target directory file and click OK to begin the scan.
Options...	Opens Advanced options.
About...	Displays information about F-Secure Internet Security 2003.

## F-Secure Internet Security 2003F-Secure Anti-Virus 2003 Windows Explorer Pop-Up Menu

You can scan disks, folders and files for viruses with 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 pop-up menu, select Scan Folders for Viruses. The *Manual Scan* window appears and scanning will be started.



If a virus is found, see *“Removing a Virus from your Computer”* on page 25.

---

**Note:** When you perform a scan, F-Secure Internet Security 2003F-Secure Anti-Virus 2003F-Secure Internet Shield 2003 uses settings for scanning from the current Virus Protection profile. See *“Changing your Virus Protection Profile”* on page 22.

---

### 3. Home

The *Home* page offers you a quick and detailed overview of your security settings and F-Secure Internet Security 2003's status.



On the Home page, you can:

- Select your Virus Protection profile, and monitor the status of your Virus Protection. For more information and instructions, see **Chapter 4. *Virus Protection***.
- Select your Internet Shield profile. For more information and instructions, see **Chapter 5. *Internet Shield***.
- Enable and disable Automatic Updates and see information on updates received by your computer. For more information and instructions, **Chapter 6. *Automatic Updates***.



## 4. Virus Protection



The screenshot shows the 'F-Secure Internet Security 2003' interface. The title bar reads 'F-Secure Internet Security'. The main window has a blue header with the product name. On the left is a navigation pane with buttons for 'Home', 'Virus Protection', 'Internet Shield', 'Automatic Updates', and 'My Subscription'. The 'Virus Protection' button is selected. The main area is titled 'Virus Protection' and shows a green checkmark icon next to the text 'Virus Protection Enabled'. Below this is a table of status information:

Virus Protection		Enabled
Virus protection profile	Medium	<a href="#">Change...</a>
Virus definitions updated	3 days ago	
Definition file created	13.12.2001 11:52	
Files scanned	12176	
Viruses removed	0	

At the bottom of the main area are two buttons: [Scan for Viruses](#) and [Advanced settings...](#). At the very bottom of the window are two buttons: [F-Secure website >](#) | [Latest virus information >](#), and [Help](#) | [Close](#).

On the Virus Protection page, you can:

- Select your Virus Protection profile (for more information, see [“Virus Protection Profiles” on page 22](#)).
- View when you have received virus definition updates, and when your virus definition files were created at F-Secure VirusLab.
- View the number of files scanned by F-Secure Internet Security 2003 and how many viruses have been removed.
- Manually scan for viruses (to learn more, see [“Scan for Viruses” on page 23](#)).

## 4.1 Virus Protection Profiles

Virus Protection profiles allow you to instantly change your level of protection according to your needs. Profiles are automatically updated to protect you against the newest forms of malicious computer programs.

If you change any settings in a profile (from Virus Protection Advanced Settings), its name will change to User-Defined. To restore your Virus Protection profile, see [Changing your Virus Protection Profile](#) below.

### Changing your Virus Protection Profile

You can change profiles at any time depending on the security protection you need. Changing your selected profile alters the level of automated actions and reporting.

Change your profile in the Virus Protection section as follows:

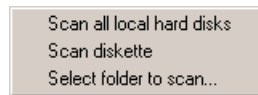
1. Click **Change**.
2. Select a profile from the drop-down list. Please read each profile's displayed description carefully before activating it.
3. Click **OK** to start using the selected profile.

## 4.2 Scan for Viruses

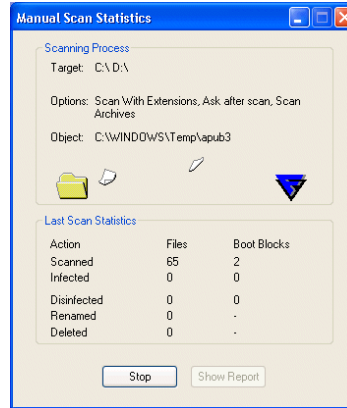
With Virus Protection enabled, your computer is protected. Opening or closing a file will automatically cause it to be scanned for viruses.

If you suspect that a certain file contains a virus, you may scan a file or your computer for viruses. To perform a scan yourself, do the following:

1. Click **Scan for Viruses**.
2. From the menu, select to scan all local hard disks, a single diskette or a folder that you will need to specify.



3. The *Manual Scan Statistics* window is displayed and shows you statistics for the scan. Click **Stop** to interrupt the scan at any time.



4. A report is generated after the scan is completed. Click Show Report to view the report in your Web browser. If a virus is found, see ["Removing a Virus from your Computer"](#) on page 25.

---

**Note:** When you perform a scan, F-Secure Internet Security 2003 uses settings from the current Virus Protection profile. To select a different profile, see ["Virus Protection Profiles"](#) on page 22.

---

## **4.3 Removing a Virus from your Computer**

### **How F-Secure Anti-Virus Disinfection Wizard Removes a Virus**

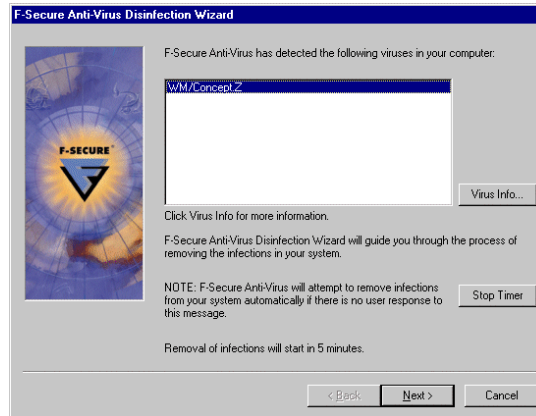
You will see the F-Secure Anti-Virus Disinfection Wizard if:

- A virus was found during a virus scan.
- A virus has been found and your virus protection profile is set to display all findings and report to you before disinfection.
- A virus was found during an automated scan (Automatic Protection is enabled) and F-Secure Internet Security 2003 was unable to remove the virus by itself.

The following steps will assist you in removing the virus.

### **Step 1 - Virus Detected**

The name of the detected virus is displayed as shown below. To proceed with the virus disinfection, click **Next**.



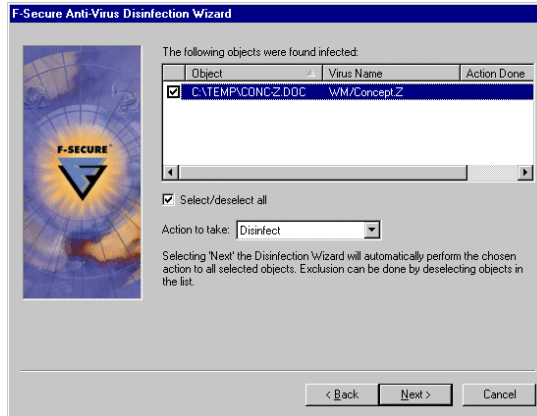
---

**Note:** For more information about the virus, click on the name of the virus, and click Virus Info. If the virus is new, it may not be described here yet. Check the F-Secure Computer Virus Info Center at <http://www.f-secure.com/v-descs/> for the latest information.

---

## Step 2 -Action Taken

A list of infected files is displayed.



In the Action to Take box, choose the action to be taken on the infected. An overview of each action is found in the table below.

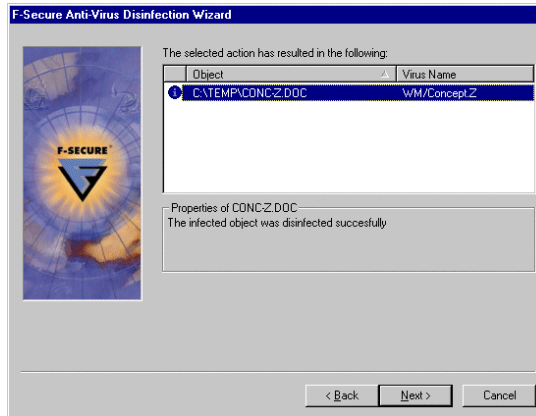
Action	Explanation
Disinfect	The Disinfection Wizard disinfects the infected file. <b>Note:</b> If Disinfection Wizard is not able to disinfect the file, it will try to rename the file automatically.
Delete	The Disinfection Wizard deletes the file that contains the virus. All information in the file will be lost. <b>Warning:</b> If you select Delete, the object that is infected will also be deleted.
Rename	The Disinfection Wizard renames the file so it will not be possible to automatically run that file. This prevents the virus from being activated.

Once you have selected the action to take, click Next and Disinfection Wizard will perform the action automatically on all of the selected objects.



### Step 3 - Action Results

The results of the action are displayed. If you chose an action that failed, you can go back and repeat step 2 and choose a different action.



If disinfect and delete actions fail, you can optionally choose to rename the file. This is typically a good idea with executables (.exe) that are infected, as renaming will alter the extension to that of a file that is not allowed to run automatically.

Please note that if disinfecting failed, Disinfection Wizard may have renamed the file automatically already (see the Action table above). You will see a note about this in the *Properties* field.

---

**Note:** In case a new virus is discovered, virus definitions are outdated or you receive a false alarm, disinfection or deletion may fail. For instructions on what to do in such a case, see [“Removing a Virus When Disinfection Wizard Fails”](#) on page 32.

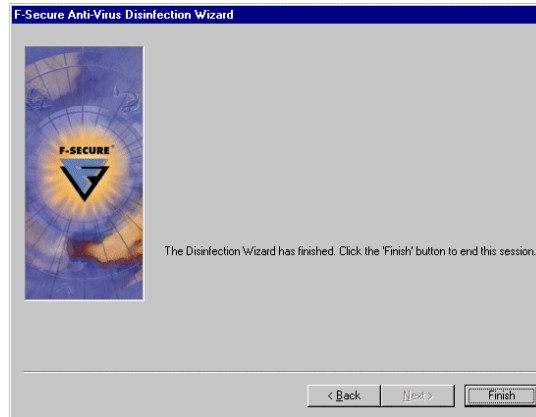
---

If the operation was successful, click **Next** to continue.

***Step 4 - Review and Finish***

A Disinfection Report will be generated after you have finished the disinfection process. If you do not want a report to be generated, clear the Generate Report check box. Please note that the Disinfection Report will not be generated for viruses that were found during an automated scan.

Click **Finish** to exit the Disinfection Wizard.



The disinfection report is displayed in your default Web browser and contains links to corresponding virus descriptions in the Web Club's virus database.

---

**Note:** If the virus was found in a file that was locked by another process at the time Disinfection Wizard tried to remove it, a window will be shown that requests to restart the computer. If you see this window, save all open documents and proceed according to the instructions stated in the window.

---

## Removing a Virus When Disinfection Wizard Fails

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

- Virus definition database is outdated. Please make sure you have the latest definition files and retry (see **Chapter 6. [Automatic Updates](#)** ).
- False alarm. Every care is taken to ensure that F-Secure Internet Security 2003 does not think that a harmless file is infected but due to the complex nature of files, F-Secure Internet Security 2003 may suspect a safe file.
- Manual disinfection is required. In some cases you need to run a tool that disinfects the file and removes the virus. This is often the case with more modern viruses that use advanced techniques to hide and attach themselves to your files.
- You have discovered a new virus. A new type of virus may have infected your computer. Don't panic. Your files are currently safe as F-Secure Internet Security 2003 detected and stopped the virus before it caused any damage.

If you are certain that the file is safe, you can ignore the warnings. You can configure Automatic protection and Manual scanning to ignore this file in future scans. To do this, see "[Setting Protection to Ignore/Scan Selected Files](#)" on page 34.

### ***How to Manually Remove the Virus***

1. Try to disinfect the file yourself. To help you remove the virus, you can either:
  - Check the F-Secure Computer Virus Info Center at <http://www.f-secure.com/v-descs/> for information on the virus. The virus information will help you remove the virus and may include a link to the tool necessary to remove the virus.
  - Advanced users: Go directly to <ftp://ftp.europe.f-secure.com/anti-virus/tools/> to find a disinfection tool that can assist you.

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

2. If you have tried Disinfection Wizard without success, your virus definition database is up-to-date and you have not been able to successfully use any disinfection tools from the F-Secure tools Website, follow the instructions in *“What if you Suspect you Have Found a New Virus?”* on page 33.

## **4.4 What if you Suspect you Have Found a New Virus?**

If F-Secure Internet Security 2003 warns you that you have a file infected with a virus, but is unable to give you a virus name, and is also unable to disinfect or remove the virus, it may be a brand new virus. Until you know that the possible virus has been removed, or that it was a false alarm, you should not attempt to use the file.

To remove the virus, follow these steps:

1. Make sure that your virus definition database is up to date. A newer definition file may tell F-Secure Internet Security 2003 how to deal with the virus in removing it from your computer.
2. If you already have the newest virus definitions (see **Chapter 6. Automatic Updates.** ), check the F-Secure website to see if there are any tools that you can use to remove the virus manually (<http://www.f-secure.com/v-descs/> or <ftp://ftp.europe.f-secure.com/anti-virus/tools/>).
3. If the previous steps fail, send the file to F-Secure VirusLab. For instructions, go to: <http://www.f-secure.com/support/technical/general/samples.shtml>.

## 4.5 Setting Protection to Ignore/Scan Selected Files

In certain cases you may want to set Virus Protection to ignore files of certain types, or to ignore specific files. This can be in cases where:

- You are certain a file is not infected, but you are receiving false alarms.
- Your computer has limited resources and setting Virus Protection to scan all files would slow down your computer to an unusable speed.
- The file is of a type that is never infected by a virus.

Some profiles already set automated scanning to scan certain file types. This offers a good balance of scanning files where viruses are typically found without taking up excess processor time and memory.

---

**Warning:** Setting Virus Protection to ignore particular files leaves these files open to future attack by viruses and limits a virus scan's ability to find and disinfect viruses. It is recommend for extreme cases only.

---

### ***Setting Real-Time Protection or Manual Scanning to Scan Selected Files***

To set Real-Time Protection or Manual Scanning to scan selected files:

1. Open the F-Secure Internet Security 2003 main window.
2. Select the Virus Protection page and click on Advanced Settings. In the Real-Time Protection and Manual Scanning tabs, make sure that Files with these extensions is checked.

### ***Setting Real-Time Protection or Manual Scanning to Ignore Selected Files***

To set Real-Time Protection or Manual Scanning to ignore selected files:

1. Open the F-Secure Internet Security 2003 main window.
2. Select the Virus Protection page and click **Advanced Settings**. In the Real-Time Protection and Manual Scanning tabs, make sure that:
  - Exclude files with these extensions is checked and enter the file extensions into the text box.
  - Exclude Objects (files, folders...) is checked. Click **Select** to browse to the files you wish to exclude and add them to the list of files to exclude.





## 5. Internet Shield



The screenshot shows the 'F-Secure Internet Security 2003' window. The title bar reads 'F-Secure Internet Security 2003'. The main header area displays 'F-Secure Internet Security 2003' over a globe background. On the left is a navigation pane with buttons for 'Home', 'Virus Protection', 'Internet Shield' (selected), 'Automatic Updates', and 'My Subscription'. The main content area is titled 'Internet Shield' and shows a green checkmark icon next to 'Internet Shield' which is 'Enabled'. Below this is a table of settings:

Setting	Value	Action
Internet shield profile	Normal security(ENG)	<a href="#">Change...</a>
Application control	Prompt	<a href="#">Change</a>
Applications allowed/denied	2 / 0	<a href="#">Change...</a>
Alert configuration	Log only	<a href="#">Change</a>
Recent alerts	3125 since yesterday	<a href="#">View...</a>
Latest alert	Today, 16:20	<a href="#">Details...</a>
Packets dropped	300291	

At the bottom right of the settings area is a link for [Advanced settings...](#). Below the settings table are links for [www.F-Secure.com >](#), [Latest virus information >](#), and [Support >](#). The bottom of the window features the F-Secure logo on the left and 'Help' and 'Close' buttons on the right.

On the Internet Shield page, you can:

- Select your Internet Shield profile (for more information, see [“Internet Shield Profiles”](#) on page 38).
- Change the status of Application Control. To do this, click **Change** beside the current Application Control status.
- Check how many applications are allowed or denied to connect to the Internet. To change an application's connection rights, see [“Changing an Application's Connection Rights”](#) on page 40.
- Change your alert configuration. To do this, click **Change** beside the current status.
- See how many alerts you have received since the specified date. Click **View** to see a list of the alerts.
- Check how many packets have been dropped. Known, dangerous packets are always dropped by Internet Shield, but you can also affect packet-dropping by customizing your Internet Shield rules (for instructions, see [“Customizing Internet Shield Rules”](#) on page 43).
- Check when you received the latest Internet Shield alert. Click **Details** to see the details of the latest alert and the top five blocked protocols and hosts (IP addresses).

## 5.1 Internet Shield Profiles

Profiles for Internet Shield allow you to instantly change your level of protection according to your needs, and are automatically updated to ensure that you are protected against the newest forms of malicious computer programs and Internet attacks.

## Changing Your Internet Shield Profile

You can change profiles at any time depending on the security protection you need. Changing your selected profile alters the level of automated actions and reporting.

Change your profile in the Internet Shield section as follows:

1. Click **Change**.
2. Select a profile from the drop-down list. Please read each profile's description before activating it.
3. Click **OK** to start using the selected profile.

To customize a profile, see [“Customizing Internet Shield Rules” on page 43](#).

## 5.2 Using Application Control

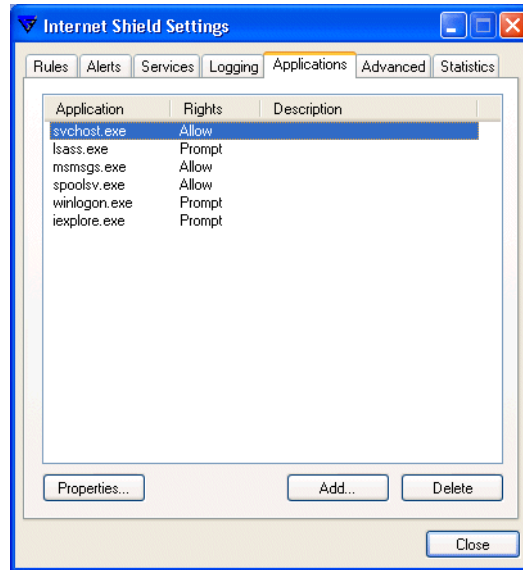
Application Control is a feature of F-Secure Internet Security 2003 that checks all applications connecting from your computer to the Internet. Application Control asks you whether the application's connection attempt should be allowed or denied, as described in [“What to do When the Application Control Pop-Up Appears”](#) on page 9. Safe and known applications should be allowed to connect to the Internet and untrusted applications should be denied connection.

A file named Action Log records all connections and their properties to allow you to see where your computer has connected. To access it, click **Advanced Settings**, then the *Logging* tab.

## Changing an Application's Connection Rights

If you want to change an application's connection rights or properties, do as follows:

1. Go to the Internet Shield page, and click **Change** beside *Applications allowed/denied*.
2. The *Internet Shield Settings* page will open.



3. Select the application whose properties you want to change (the current Rights are listed in the Rights column). Click **Properties**.
4. Select Deny, Prompt or Allow. Click **OK** to return to the Applications page.
5. The application's new rights will be listed in the Rights column beside the application's name. Click **Close** to finish.

### **What can be Considered "Safe"?**

- A known application that you have actively started yourself.
- Windows services that are connecting to the Internet.

### ***Safe Microsoft Windows Services***

Certain Microsoft Windows services require network access in order to function. Most of the services are allowed automatically but Application Control may prompt the services listed below, especially on Windows NT 4.0, Windows 2000 and Windows XP platforms. Please allow these to access network, otherwise some of the Windows functionality may fail."

Application list:

---

**Note:** %Winnt% refers to Windows installation directory, typically C:\Winnt\  

---

<b>Executable</b>	<b>Location</b>	<b>Description</b>	<b>Network Traffic</b>
SVCHOST.EXE	%Winnt%\System32\	Generic Host Process for Win32 Services	udp/67 out, udp/68 in, udp/137 out
SPOOLSV.EXE	%Winnt%\System32\	Spooler Subsystem App	udp/137 out, udp/138 out
LSASS.EXE	%\Windows%\System32\	LSA Executable and Server DLL	udp/137 out
SERVICES.EXE	%Winnt%\System32\	Services and Controller app	udp/67 out, udp/68 in, udp/137 out
WINLOGON.EXE			udp/137 out

## What can be Considered "Unsafe"?

Any application you have received from a distrusted source should always be treated with suspicion. Any application you have received from a trusted source without prior agreement should also be treated as suspicious.

- Any application you have not actively installed yourself, or have no knowledge of.
- An application you consider safe, but which is attempting a connection without you starting it.
- A connection that does not have a proper target name (text web address) in it.

## 5.3 Customizing Internet Shield Rules

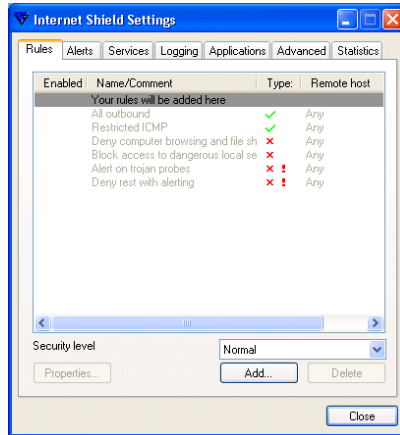
There may be situations where you wish to add, change or delete rules that define what to do with certain connections. Such situations could be when you want to:

- Connect to a new game server on a particular computer.
- Allow general connections, but block a connection to a particular website or computer that you do not trust.

To customize your Internet Shield settings:

1. Click **Advanced Settings** on the Internet Shield page. The Advanced Settings window opens.
2. From the Security Level pull-down menu, select the profile you want to customize.

3. Click the Rules tab (if it is not already selected).



- To change an existing rule, select the rule from the list and click **Properties**.
- To add a new rule, click **Add**.
- To delete a rule, select the rule from the list and click **Delete**.

---

**Note:** It is not possible to change or delete preset rules. You can only add new rules, or change and delete rules that you have added yourself.

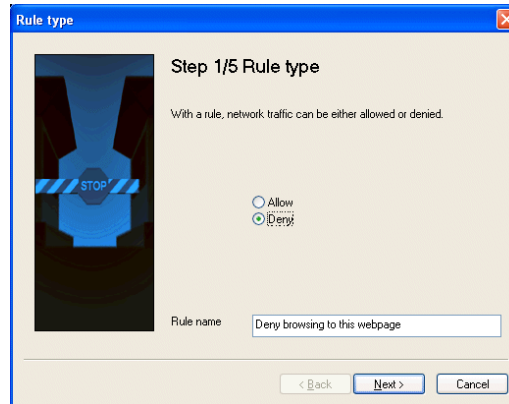
---



## Creating a New Internet Shield Rule

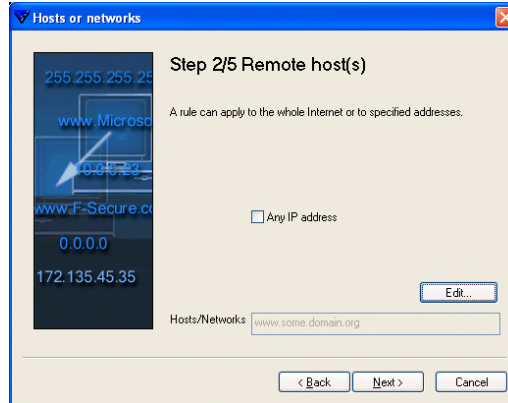
### ***Step 1 - Rule Type***

Give the rule a descriptive name and choose to either allow or deny the connection.



## Step 2 - Specify the target(s)

Choose whether to apply this rule to all connections or to selected connections only.



You can either:

- Check Any IP Address to apply the rule to all Internet connections, and click **Next** to continue to step 3, or
- Uncheck Any IP address and click **Edit** to open a new window where you can enter the details about the targets.

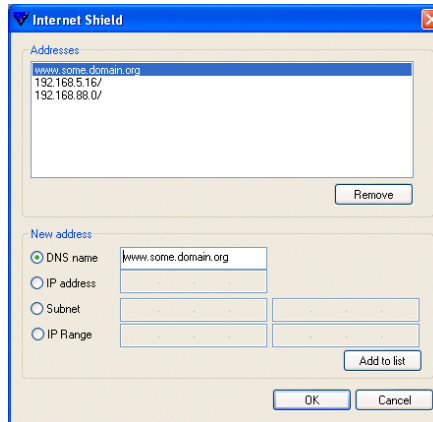
- Targets can be listed in any order and type and can be any DNS name, IP address, subnet (in bit net mask format) or IP address range. For example:

DNS name:                      www.some.domain.org

IP address:                     192.168.5.16

Subnet:                         192.168.88.0/29

IP range:                        192.168.1.1-192.168.1.63

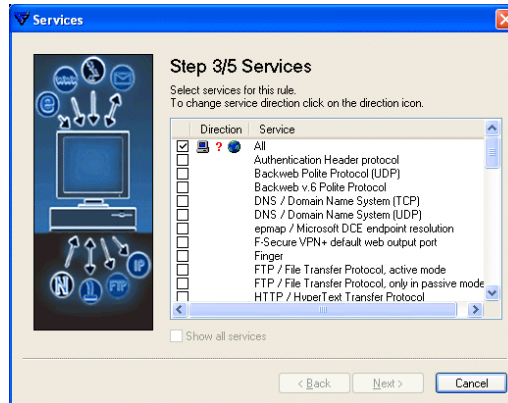


Click **Add** to list to add your new target to the list of targets to which this rule applies. To remove a target address, select it from the list and click **Remove**. To edit a target's properties, select the target address from the list. Click **OK** to return to the Remote host(s) page and click **Next** to continue.





### **Step 3 - Choose the Service and Direction for the Rule**

Choose the service for which this rule will apply, from the list of available services. If you want the rule to apply to all services, select *All* from the top of the list.

You can select as many individual services as you want.

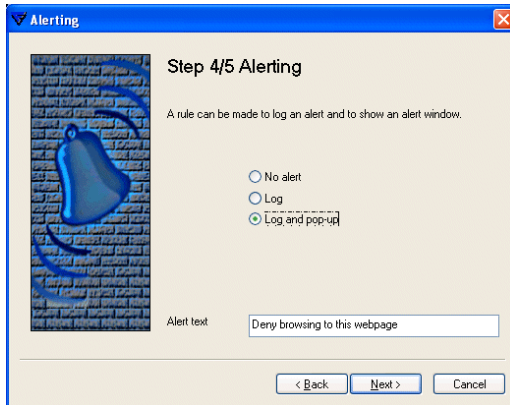


For the chosen services, select the direction in which the rule will apply by clicking on the red question mark that appears. Repeated clicks cycle between the available choices. See the table below for examples.

Selection	Term	Explanation
	Undefined	The direction has not yet been defined. Click the graphic to define a direction.
	Incoming	The service will be allowed /denied if coming from the Internet to your computer.
	Outgoing	The service will be allowed /denied if going from your computer to the internet.
	Both	The service will be allowed /denied to/from your computer in both directions.

#### **Step 4 - Choose the Logging and Reporting**

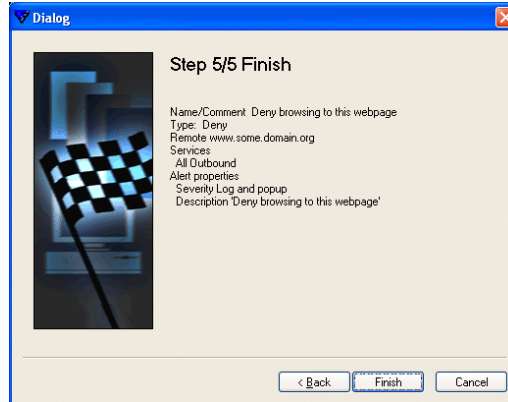
You can select whether you want to be informed whenever the rule is applied to an attempted connection.



- *No alert* means that you receive no information when the rule is applied to a connection.
- *Log* means that data about the connection is logged to a file.
- *Log and pop-up* means that data is logged and you receive a notification pop-up window for example when the connection is allowed/denied.

### **Step 5 - Review and Accept the Rule**

You can review your rule now. Click **Back** through the rule to make any needed changes.



If you are satisfied with your new rule, click **Finish**. Your new rule will be added to the top of the list in the active set of rules on the Rules tab of Internet Shield settings.

## 5.4 Advanced Settings

---

**Note:** This section is only for expert computer users. Internet Shield may be disabled by changing settings.

---

To access advanced Internet Shield settings, click **Advanced Settings** on the Internet Shield page. Click the Advanced tab in the window that appears.

The following items should be considered when customizing Internet Shield's advanced settings.

### **Trusted Interface**

Trusted Interface can be used if the computer with F-Secure Internet Security 2003 installed acts as a network gateway, e.g. Windows Internet Connection Sharing is enabled. The network interface used for local networking can be set to "Trusted Interface", so that no Internet Shield rules are applied to that interface.

---

**Note:** This network interface will be left completely open and is not protected.

---

### **Packet Filter**

Packet filtering is the main function of Internet Shield, and disabling it will leave it mostly ineffective against all types of network attacks.



## **Application Control**

Do not disable Application Control from the Advanced Settings window. Disabling (unchecking) Application Control increases the risk of software-based attacks, and should not be done unless needed for troubleshooting etc.

If you want to disable Application Control, go to the Internet Shield page and change Application Control's status from *Prompt* to *Allow and log*.



## 6. Automatic Updates

The automatic update service activates transparently in the background any time you connect to the Internet, and ensures that you receive the latest updates transparently to your computer.



In the Automatic Updates section, you can:

- Click **Enable** to activate or **Disable** to deactivate Automatic Updates.
- See when the most recent update check was made and/or when the next update check will take place.

If you want to personally check that you have the latest virus definitions, click **Check Now**. If your definitions are not up to date, the newest versions will be downloaded.

---

**Note:** 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.

---

---

**Note to 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 use the **Check now** button to check for updates.

---

- Check when each of the three features below has been updated.

Virus definitions	Frequently updated database for virus protection. These automatic updates are performed transparently in the background without you needing to do anything, and activate any time you connect to the Internet.
Security Profiles	Various levels of security settings. To maximize the protection of your computer, profiles are updated whenever new types of attacks are discovered.
Software	F-Secure Internet Security 2003 software updates that are downloaded in the background.



## 7. My Subscription

The My Subscription page displays information about your personal subscription.



On the My Subscription page, you can:

- View your subscription status. The expiry date of your subscription is stated with the current status as well as one of the following status icons:



Valid

Your subscription is valid.



About to expire

Your subscription is valid but is about to expire.



Expired

Your subscription has expired.

- Renew your subscription online (or if you are using an evaluation version, you can buy a new subscription).
- Change your subscription number.



## 8. How F-Secure Internet Security 2003 Protects Your Computer

### 8.1 Viruses Protection

Malware (from "malicious software") is the term used for several forms of programming or files such as viruses, worms, Trojan horses, jokes and hoaxes that are developed for the purpose of doing harm to your computer.



Virus Protection detects and removes viruses and other malicious computer programs from your computer. Whenever a file is accessed, either from your own computer's hard drive, an external storage device or the Internet, F-Secure Internet Security 2003's Virus Protection checks the opened file for viruses.

Up-to-date virus protection software is combined with automatically updated virus definitions to offer you the best possible protection against viruses. The F-Secure Anti-Virus research laboratory regularly publishes and updates virus definitions, profiles and the F-Secure Internet Security 2003 software that are quickly and automatically downloaded by F-Secure Internet Security 2003 whenever you connect to the Internet.

F-Secure Virus Protection uses multiple virus scanning engines to ensure flawless protection against viruses. Of these, the heuristic scanning engine protects especially against new and unknown viruses.

## 8.2 Internet Shield

Whenever your computer is connected to the Internet, it is a target for Internet attacks from unknown sources. In some cases these attacks are not really attacks as such, but harmless messaging that has accidentally arrived at your computer. In other cases however, an unknown person or computer is deliberately trying to access your computer and files.

Your computer's security can be compromised in several ways, including the following:

- Services inadvertently left open can easily be found and abused by outsiders.



Internet Shield protects your computer while you connect to the Internet. It allows only those connections to and from your computer that are stated in your selected profile. All other traffic is not allowed, effectively decreasing a hacker's chances of viewing/changing information on your computer.

- Your computer broadcasts information about itself. When it is connected to the Internet, anyone who knows how to read this information can use it as a basis for an attack against you.



Internet Shield stops your computer from broadcasting information about itself on the Internet as well as any outgoing connections that try to leak information about you or your computer.

- Some Trojan horses hide themselves inside software that you normally trust. They use a connection or application that you think is safe to transfer data about you or your computer.



Internet Shield recognizes attempts by Trojan Horses to transfer data, and prevents the connection from occurring, therefore ensuring your data is protected at all times from unwanted attacks.

### **8.3 How Can You Help to Avoid Viruses and Other Malware**

Using F-Secure Internet Security 2003 is the best line of defence against viruses as it stops any known virus before it infects your computer. However, you can help to protect your computer:

- Keep your operating system and applications up-to-date and apply the latest patches when they become available. Be sure to get the updates directly from the vendor.
- Always save files you download to your hard disk before opening or running them. Saving a file that you have downloaded ensures that F-Secure Internet Security 2003 checks it.

- Most worms use email to spread and are targeted at users of Microsoft Outlook or Outlook Express. If you need to use any version of Outlook, regularly check for, download and install the latest Outlook security patch from Microsoft.
- When you receive email advertisements, other unsolicited email, or if you feel that an email you received from a friend is somehow strange, do not open their attachments or follow the web links they quoted. If you do want to see an attachment, save it to your hard disk before opening it. This ensures that F-Secure Internet Security 2003 checks the attachment for viruses.
- Avoid files from public newsgroups and online chat systems such as IRC and ICQ.
- Avoid forwarding virus warnings or chain letters that you receive from others.

# Troubleshooting

## Installation

### **Q. Installation failed. What happened?**


A. If there was no Internet connection, F-Secure Internet Security 2003 was unable to validate your subscription. Make sure you have an Internet connection and install F-Secure Internet Security 2003 again.

## General Use

### **Q. F-Secure Internet Security 2003 is very slow and/or does not open. What's wrong?**

A. Internet Explorer 3.0 or newer may not be installed. See if you have Internet Explorer installed and check the version number (Internet Explorer is available from the Microsoft Corporation Web site).

### **Q. I can't see the F-Secure Internet Security 2003 icon in the system tray at the bottom right corner of the screen.**

A. In Windows XP, icons may be hidden. To show the hidden icons, click the  button. If you are not using Window XP, install F-Secure Internet Security 2003.




## Virus Protection

**Q. F-Secure Internet Security 2003 is not able to disinfect/delete/rename an infected file on my computer. What do I do?**

A. See *“Removing a Virus When Disinfection Wizard Fails”* on page 32.

**Q. I am installing software, but Virus Protection informs me there is a virus in it and because of this I cannot complete the installation.**

A. If you are certain that the software does not contain any viruses, you can do one of the following:

- Choose a less strict Virus Protection profile (for instructions, see *“Changing your Virus Protection Profile”* on page 22), or
- Right-click the  icon in the system tray (at the bottom right hand of your screen) and choose *Unload F-Secure products*. Don't forget to reload products after installation is complete.



## Internet Shield

**Q. (I think) I am being attacked by a hacker from the Internet. What do I do?**

A. Go to the Internet Shield page and select the Block All profile. For more information on selecting an Internet Shield profile, see *“Changing Your Internet Shield Profile”* on page 39.

### Application Control

**Q. How can I change the application's connection rights to the Internet? How can I allow a previously denied application to connect to the Internet?**

A. See *“Changing an Application's Connection Rights”* on page 40.

**Q. My email program (or another program such as the Internet browser) stopped working.**

A. You may have accidentally denied the program from connecting. See *“Changing an Application's Connection Rights”* on page 40 for information on allowing the program to connect.

**Q. What programs/applications can be allowed to connect to the Internet?**

A. See *“Using Application Control”* on page 39 to help you decide which applications you should allow (or deny) a connection.



## Automatic Updates

**Q. What if my computer is offline when an automatic virus update is due?**

A. The next time you are online, F-Secure Internet Security 2003 will download the latest automatic virus update.

**Q. How often should the virus definition databases be updated?**

A. Virus definition databases are updated automatically if the Automatic Updates feature is enabled. If you would like to update the databases manually, you should do so at least once a week.

**Q. I am trying to manually check for virus definition database updates (clicking Check Now) but nothing happens.**

A. If you are using a modem or have an ISDN connection, you are required to connect to the Internet manually before clicking **Check Now**.



# **Glossary**

## **Application**

A software program written for a specific purpose. Applications normally need to be manually launched.

## **Application Control**

Application Control is a feature of F-Secure Internet Security 2003 that automatically checks an application connecting from your computer to the Internet by comparing the application with lists of safe (pre-approved) software and known malicious software (Trojans etc.).

## **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.

## **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 "handle" for an Internet address. The Internet address [www.some.domain.org](http://www.some.domain.org) is an example of a DNS name.

**Heuristic**

Exploratory problem-solving that utilizes self-educating techniques.

**Malware**

Malware (from "malicious software") is programming or files that are developed for the purpose of doing harm. This includes computer viruses, worms and Trojan horses.

**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 email 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.

**Profile**

Profiles are preconfigured attributes that set your level of security. They are automatically updated to ensure that you are protected against the newest forms of malicious computer programs and Internet attacks.

**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.

## **Trojan Horse**

A program that intentionally does something that the user of the program does not expect.

## **Virus**

A computer program that spreads by replicating itself.

## **Virus Definition Database**

Virus Definition Databases are used to detect viruses. Whenever a new virus is found, the databases need to be updated for virus protection to be able to detect that virus.

## **Worm**

A computer program capable of replication by inserting copies of itself in networked computers.



## **Support and Maintenance**

During the license period, which is equal to your subscription period, you are entitled to standard support and maintenance services provided by F-Secure or an F-Secure service provider partner. After the termination of the license, the rights to all services including virus definition database updates are expired and the software may automatically disable its operation unless you renew your license. Please contact your license provider for more information.

### **Did you Purchase the Service from an Internet Service Provider?**

If you purchased the service from an Internet Service Provider, you will automatically receive software upgrades and virus definition database updates to your computer. For information on technical support and other maintenance services, please see your service agreement with your Internet Service Provider.

### **Did you Purchase the Service from a Retail Store or F-Secure Online Store?**

If you purchased the service from a retail store, please register your license by filling out the registration form included in the box or on the F-Secure website at: <http://www.f-secure.com/register/>.

By registering your license, you will have access to F-Secure support and maintenance services. If you purchased the service from F-Secure online store, you are automatically registered.

## Technical Support

F-Secure's Online Support Center offers you a comprehensive collection of technical documents that provide you with solutions for problem-based questions, most common installation problems and virus removal instructions. If you have any problems or questions that are not covered in the manual or online services, please contact the F-Secure support staff.

### ***F-Secure Online Customers:***

Online Support Center: <http://www.f-secure.com>

Email: [eStore@F-Secure.com](mailto:eStore@F-Secure.com)

### ***Finland:***

Online Support Center: <http://www.f-secure.fi/fin/>

Email: [Anti-Virus-Support@F-Secure.com](mailto:Anti-Virus-Support@F-Secure.com)

Phone: +358 9 2520 5050

### ***Sweden:***

Online Support Center: <http://www.f-secure.se/support/>

Email: [FSAV-Support@F-Secure.se](mailto:FSAV-Support@F-Secure.se) (antivirus)

[FSIS-Support@F-Secure.se](mailto:FSIS-Support@F-Secure.se) (Internet Security)

Phone: +46-8-507 440 11 (toll free)

***Other countries:***

Online Support Center: <http://www.f-secure.com/support/>

Email: [Anti-Virus-Support@F-Secure.com](mailto:Anti-Virus-Support@F-Secure.com)

Phone: +358 9 2520 5050

## **Maintenance**

Virus definition databases are automatically updated to your computer during the subscription period. If you have registered your license, F-Secure may from time to time provide you, at no additional cost, with new software versions, service packs and hot fixes which you can download from F-Secure web site. For a comprehensive collection of virus-related information, please visit F-Secure website at: <http://www.f-secure.com/virus-info/>.