WSKA

wska.com

F-Secure Internet Security 2003

Français | English | Deutsch

Table of Contents

Table des matières

Inhaltsverzeichnis

F-Secure Internet Security 2003

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

User's Guide

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 35.

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. Depending on your installation method, either:
   - 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.
   - Download the product package to your computer. Close all other programs and execute the product package to start installation.
2. 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.
3. Choose the language you want to use for this installation and click **Next** to continue.
4. 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.
5. Choose the directory to which you want to install F-Secure Internet Security 2003. Click **Next** to continue.
6. 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.

If you are downloading components from the Internet, wait until the network installer has downloaded all the packages. This typically takes from less than twenty minutes with an ADSL connection up to about an hour or more with a fast modem.

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 8.

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 7.

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 41). 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 24).

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 24.

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.

Icon	Meaning	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 tool-tip. Enable the feature that is currently disabled or go to F-Secure Internet Security 2003 and check for updates.
	Unloaded. F-Secure Internet Security 2003 is deactivated and your computer is not protected.	Right-click the  icon and select *Reload* 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.

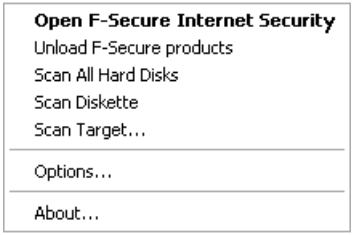
To open F-Secure Internet Security 2003, double-click the icon with your left mouse button.

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.



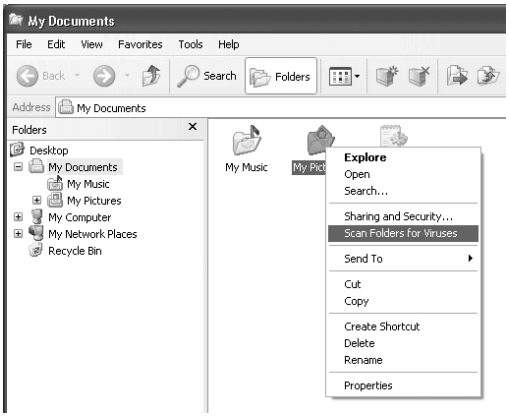
To get a better understanding of each of the menu items, see the table below:

Selection	Explanation
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.

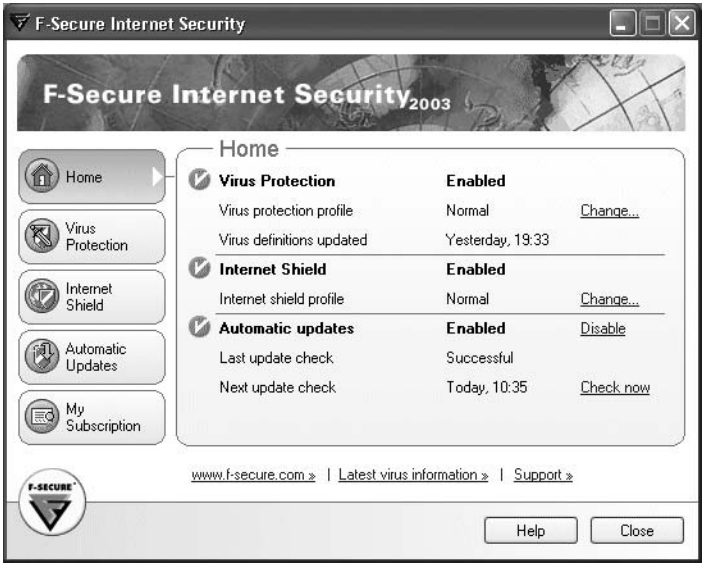


If a virus is found, see *"Removing a Virus from your Computer"* on page 17.

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 16.

3. Home

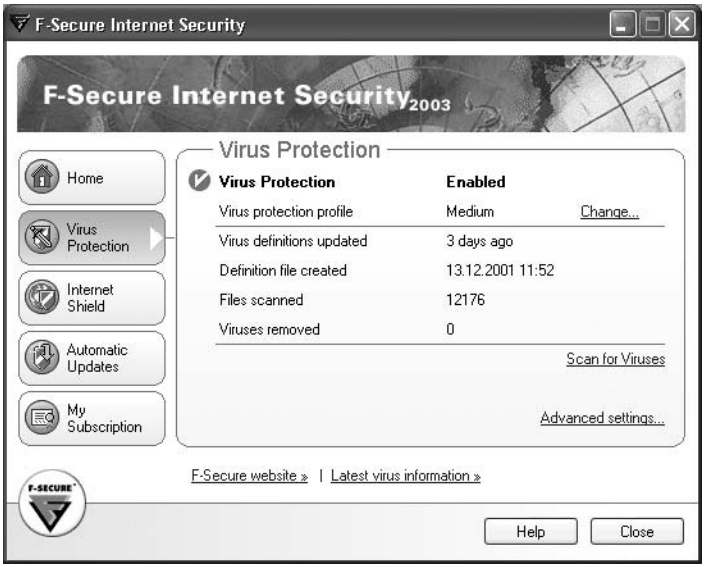
The *Home* page offers you a quick and detailed overview of your security settings and F-Secure Internet Security 2003's status.



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



On the Virus Protection page, you can:

- Select your Virus Protection profile (for more information, see *"Virus Protection Profiles"* on page 15).
- 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 16).

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.

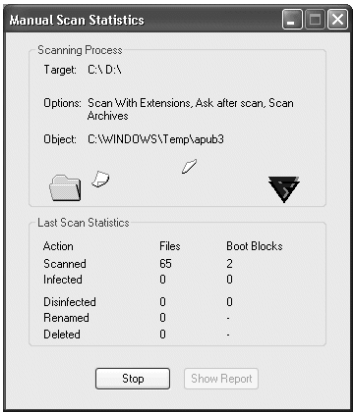
4.2 Scan for Viruses

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 17.

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 15.

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.

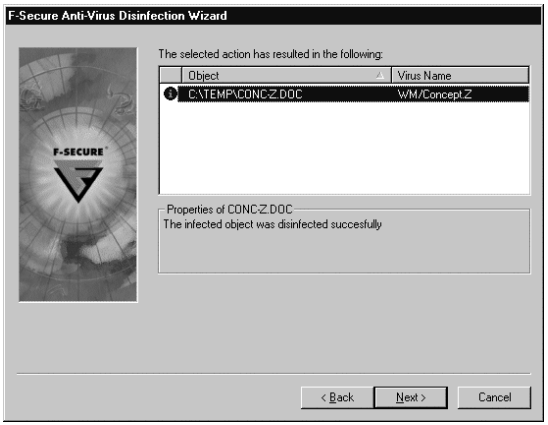
In the Action to Take box, choose the action to be taken on the infected. An overview of each action is found in the table below.

Action	Explanation
Disinfect	The Disinfection Wizard disinfects the infected file. **Note:** 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. **Warning:** 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 20.

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 21.

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 21.

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:

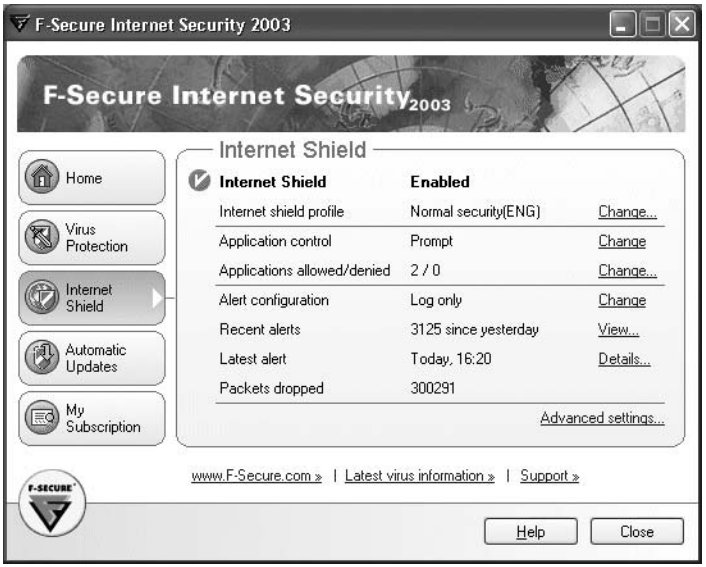
1. Open the F-Secure Internet Security 2003 main window.
2. Select the Virus Protection page and click on Advanced Settings. In the Real-Time Protection and Manual Scanning tabs, make sure that Files with these extensions is checked.

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



On the Internet Shield page, you can:

- Select your Internet Shield profile (for more information, see *"Internet Shield Profiles"* on page 24).
- 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 24.
- 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 26).
- 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 26.

5.2 Using Application Control

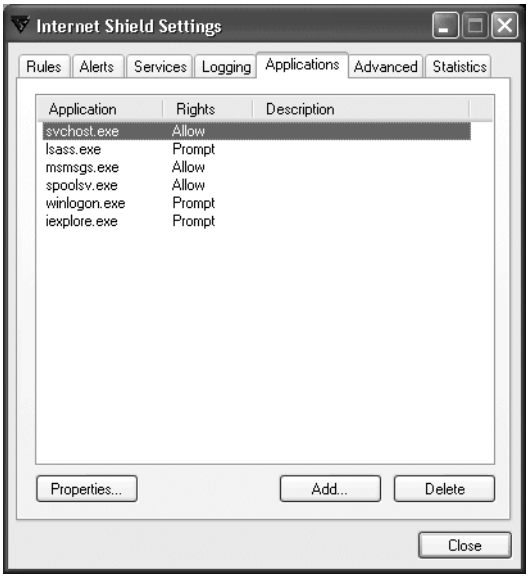
Application Control is a feature of F-Secure Internet Security 2003 that checks all applications connecting from your computer to the Internet. Application Control asks you whether the application's connection attempt should be allowed or denied, as described in *"What to do When the Application Control Pop-Up Appears"* on page 7. 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\

Executable	Location	Description	Network Traffic
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

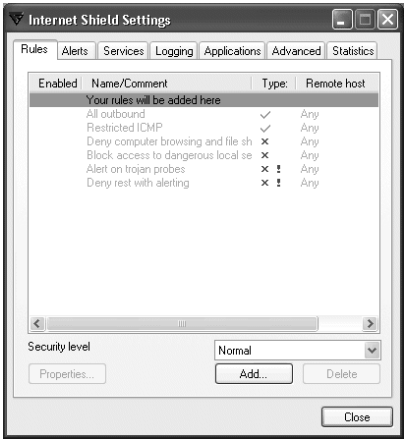
There may be situations where you wish to add, change or delete rules that define what to do with certain connections. Such situations could be when you want to:

- 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).



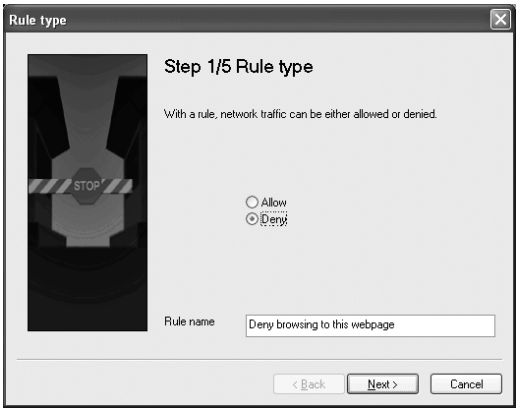
- To change an existing rule, select the rule from the list and click **Properties**.
- To add a new rule, click **Add**.
- To delete a rule, select the rule from the list and click **Delete**.

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

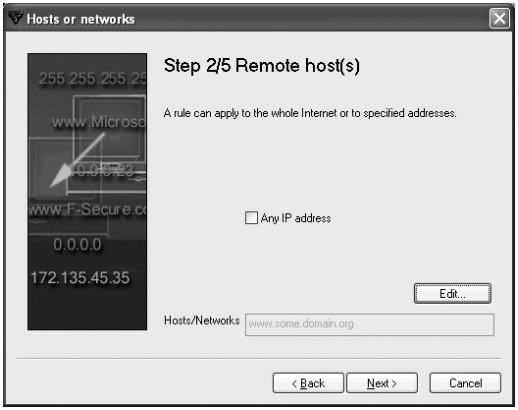
Step 1 - Rule Type

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



Step 2 - Specify the target(s)

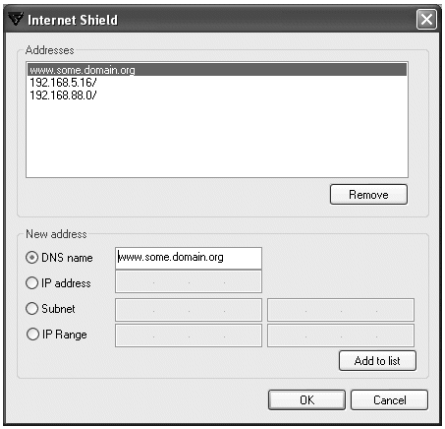
Choose whether to apply this rule to all connections or to selected connections only.



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

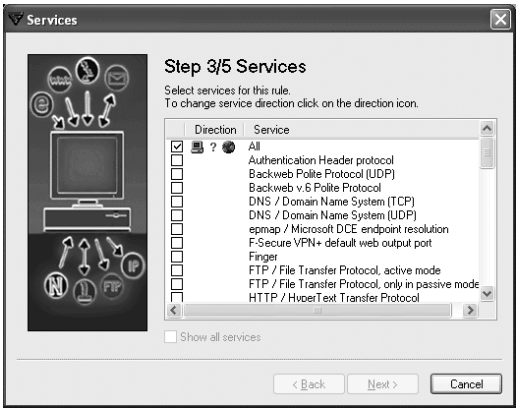


Click **Add** to list to add your new target to the list of targets to which this rule applies. To remove a target address, select it from the list and click **Remove**. To edit a target's properties, select the target address from the list. Click **OK** to return to the Remote host(s) page and click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

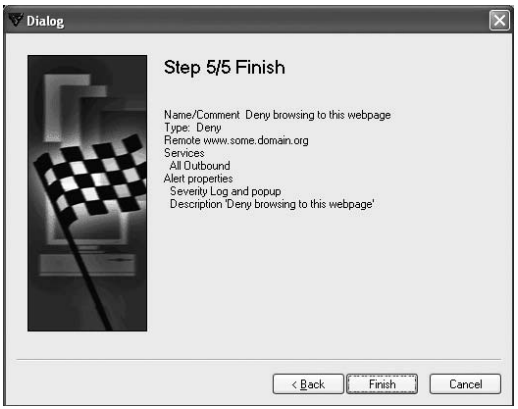
Step 4 - Choose the Logging and Reporting

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.

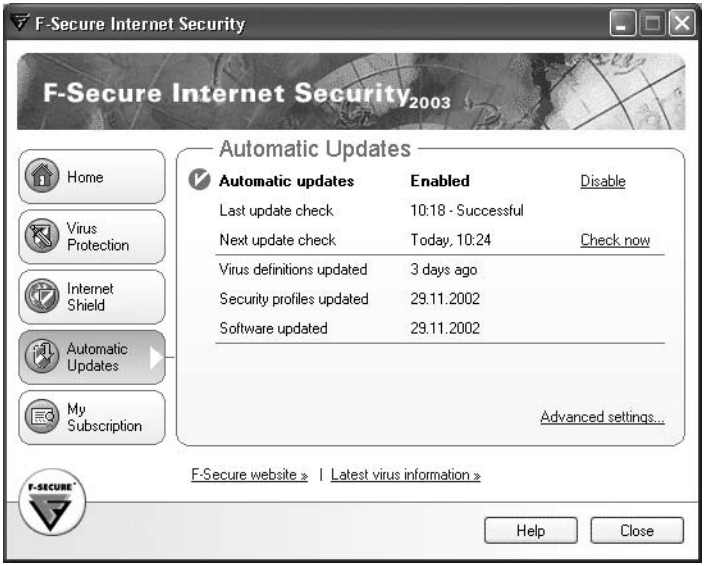
Application Control

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.

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 20.

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 16), 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 24.

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 24.

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 24 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 24 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 2003will 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 2003F-Secure Internet Shield 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 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.

English technical support

WSKA Editions

7200 The Quorum
Oxford Business Park North
Garsington Road
Oxford OX4 2JZ - Great Britain

Fax: +33 3 87.18.78.02
E-mail: uksupport@wska.com
www.wska.com

F-Secure Internet Security 2003

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

Guide de l'utilisateur

À propos de ce guide

Ce guide fournit toutes les informations dont vous avez besoin pour installer et utiliser F-Secure Internet Security 2003.

Chapitre 1. *Installation de F-Secure Internet Security 2003*. Fournit les informations nécessaires pour installer F-Secure Internet Security 2003.

Chapitre 2. *Démarrage*. Présente des informations utiles pour les nouveaux utilisateurs et constitue une référence pour les utilisateurs plus expérimentés sur l'accès et la prise en mains de F-Secure Internet Security 2003.

Chapitre 3. *Accueil*. Présente un aperçu rapide et détaillé des paramètres de sécurité et de l'état de F-Secure Internet Security 2003.

Chapitre 4. *Protection antivirus*. Explique comment vous pouvez activer ou désactiver protection antivirus, sélectionner votre profil de protection antivirus et surveiller la réception de mises à jour des définitions de virus.

Chapitre 5. *Protection Internet*. Explique comment vous pouvez modifier les profils Internet Shield, voir combien de connexions ont été autorisées ou refusées, et accéder à des paramètres avancés.

Chapitre 6. *Mises à jour automatiques*. Fournit des informations sur le service de mise à jour automatique, qui procure ce qu'il y a de plus récent en termes d'informations sur les virus, versions du logiciel et versions des profils.

Chapitre 7. *Mon abonnement*. Explique comment vous pouvez vérifier l'état de votre abonnement, renouveler celui-ci et changer de numéro d'abonnement.

Chapitre 8. *Comment F-Secure Internet Security 2003 protège votre ordinateur*. Définit les menaces qui pèsent sur un ordinateur et explique comment F-Secure Internet Security 2003 protège votre ordinateur contre ces menaces.

Dépannage - Résolution de certains problèmes courants.

Glossaire - Définition des termes.

Support et maintenance - Contacts pour l'assistance technique.

Explication des icônes

Les icônes suivantes apparaissent dans F-Secure Internet Security 2003 :

	Activé	La fonction est activée et opère correctement.
	Question	Question pouvant exiger de prendre une décision.
	Info.	Informations complémentaires pour vous aider à utiliser F-Secure Internet Security 2003.
	Occupé	Veuillez patienter.
	Avertissement	Une fonction de F-Secure Internet Security 2003 est désactivée ou vos définitions de virus n'ont pas été mises à jour récemment.
	Erreur	Une erreur s'est produite. Lisez attentivement le message d'erreur.

Remarque : Certaines icônes ont une fonction différente dans la page Mon abonnement. Pour plus d'informations, voir **Chapitre 7.** *Mon abonnement*. page page 81.

1. Installation de F-Secure Internet Security 2003

1.1 Avant de commencer

Configuration requise

Votre ordinateur doit répondre aux exigences suivantes pour que vous puissiez installer et exécuter F-Secure Internet Security 2003 :

Processeur :	Intel Pentium II ou supérieur
Système d'exploitation :	Microsoft® Windows® 95/98/ME/NT4.0 (SP6 requis)/2000/XP
Mémoire :	Windows 98/98/ME/NT4.0 - 64 Mo RAM Windows 2000/XP - 128 Mo RAM
Espace disque :	30 Mo d'espace libre sur le disque dur (60 Mo pendant l'installation)
Écran :	Minimum 256 couleurs
Connexion Internet :	Une connexion Internet est requise pour valider votre enregistrement et recevoir des mises à jour
Navigateur :	Internet Explorer 3.0 ou supérieur

Préparation de votre ordinateur en vue de l'installation

Il n'est pas recommandé d'utiliser plusieurs antivirus et pare-feu en même temps. Un conflit entre les logiciels antivirus pourrait endommager vos fichiers.

Suppression d'autres logiciels antivirus/pare-feu

F-Secure Internet Security 2003 peut automatiquement mettre à niveau F-Secure Anti-Virus 4 et 5, et F-Secure Distributed Firewall 5.

Les programmes antivirus et pare-feu d'autres fournisseurs doivent être désinstallés séparément avant l'installation de F-Secure Internet Security 2003. Consultez la documentation de votre fournisseur pour savoir comment désinstaller ces logiciels.

1.2 Procédure d'installation

Remarque : Si vous utilisez Windows NT 4.0, Windows 2000 ou Windows XP et avez plusieurs comptes, vous devez vous connecter comme administrateur pour pouvoir installer F-Secure Internet Security 2003.

Pour installer F-Secure Internet Security 2003, procédez comme suit :

1ère partie : Installation de F-Secure Internet Security 2003

1. Selon la méthode d'installation choisie, vous devez procéder comme suit :
   - Insérez votre CD F-Secure Internet Security 2003 dans le lecteur de CD-ROM de l'ordinateur.

     L'installation devrait démarrer automatiquement. Si elle ne démarre pas, accédez aux répertoires du CD et ouvrez le répertoire Setup. Recherchez le fichier install.exe et double-cliquez dessus pour lancer l'installation.
   - Téléchargez le fichier d'installation du produit sur votre ordinateur. Fermez tous les autres programmes puis exécutez ce fichier pour démarrer l'installation.
2. Fermez tous les autres programmes et insérez votre CD F-Secure Internet Security 2003 dans le lecteur de CD-ROM de l'ordinateur.

   L'installation devrait démarrer automatiquement. Si elle ne démarre pas, accédez aux répertoires du CD et ouvrez le répertoire Setup. Trouvez le fichier *install.exe* et cliquez deux fois dessus pour lancer l'installation.
3. Choisissez la langue que vous souhaitez utiliser pour l'installation et cliquez sur **Suivant** pour continuer.
4. Lisez le contrat d'abonnement et, s'il vous agrée, cochez *J'accepte le contrat*. Cliquez sur **Suivant** pour continuer.
5. Choisissez le répertoire dans lequel vous souhaitez installer F-Secure Internet Security 2003. Cliquez sur **Suivant** pour continuer.
6. Les fichiers sont transférés vers votre ordinateur. Une fois le transfert terminé, passez à la deuxième partie de l'installation.

Remarque : Vous serez peut-être invité à faire redémarrer l'ordinateur. Sélectionnez *Redémarrage immédiat* (si vous sélectionnez *Redémarrage ultérieur*, l'installation ne sera pas achevée tant que vous n'aurez pas fait redémarrer l'ordinateur) et cliquez sur **Terminer**.

2e partie : Sélection des composants et validation de votre abonnement

1. Pour valider votre abonnement, assurez-vous que la connexion à Internet est active. Vous êtes invité à choisir l'option appropriée :
   - Entrez votre numéro d'abonnement pour enregistrer celui-ci. Cliquez sur **Suivant** pour continuer.

- Choisissez d'évaluer le produit (si vous installez en mode évaluation). Cliquez sur **Suivant** pour continuer. Choisissez le type d'installation préféré dans la fenêtre qui suit, puis cliquez sur **Suivant** pour continuer.

Conseil : Vous pouvez suivre la progression de l'installation en cliquant deux fois sur  dans la barre d'état du système Windows, en bas à droite de l'écran. Cette icône sera remplacée par l'icône  une fois l'installation terminée.

Si vous téléchargez des composants depuis Internet, attendez que le programme d'installation en réseau ait téléchargé tous les fichiers d'installation. Cette opération dure généralement entre moins de vingt minutes (connexion ADSL) et environ une heure ou plus (modem rapide).

2. Une fois que F-Secure Internet Security 2003 a installé les fichiers nécessaires, vous êtes invité à faire redémarrer l'ordinateur. Sélectionnez *Redémarrage immédiat* (si vous sélectionnez *Redémarrage ultérieur*, l'installation ne sera pas achevée tant que vous n'aurez pas fait redémarrer l'ordinateur). Cliquez sur **OK** pour terminer.

   Pour vous assurer que l'installation a réussi, consultez *"F-Secure Internet Security 2003 est-il actif et fonctionne-t-il correctement ?"* à la page 54.

Remarque : Lorsque l'installation est terminée, le contrôle d'application peut vous demander d'autoriser ou non l'accès à Internet par toute application. Pour obtenir des instructions, consultez *"Que faire lorsque la fenêtre de contrôle d'application apparaît ?"* à la page 53.

1.3 Si vous devez désinstaller le logiciel F-Secure Internet Security 2003

Désinstallez F-Secure Internet Security 2003 à l'aide de la fonction *Ajout/Suppression de programmes* du panneau de configuration Windows. Cette méthode assure la suppression sûre et complète du programme. Pour ce faire :

1. Ouvrez le menu Démarrer de Windows.
2. Sélectionnez *Paramètres -> Panneau de configuration -> Ajout/Suppression de programmes*.
3. Sélectionnez *F-Secure Internet Security 2003* et cliquez sur **Supprimer**.
4. Redémarrez l'ordinateur.

2. Démarrage

2.1 Première utilisation de F-Secure Internet Security 2003

Si vous utilisez F-Secure Internet Security 2003 pour la première fois, consultez les sections suivantes, qui vous aideront à faire en sorte que F-Secure Internet Security 2003 soit actif et vous protège de manière adéquate par rapport à vos besoins de sécurité.

- Section 2.2. *Que faire lorsque la fenêtre de contrôle d'application apparaît ?*.
- Section 2.3. *F-Secure Internet Security 2003 est-il actif et fonctionne-t-il correctement ?*
- Section 2.4. *Options d'accès à F-Secure Internet Security 2003*.

2.2 Que faire lorsque la fenêtre de contrôle d'application apparaît ?

Lorsque F-Secure Internet Security 2003 est installé, la fonction de contrôle d'application peut intervenir lorsqu'une application tente de se connecter à Internet, selon votre profil Internet Shield.

Cette fonction permet de naviguer en toute sécurité et constitue une excellente défense contre les programmes malveillants tels que les chevaux de Troie (pour une définition de ce terme et d'autres concepts, voir le *Glossaire* en page 91). Au début, cependant, elle entraînera le blocage ou l'ouverture de connexions à une adresse particulière. Le nombre de demandes diminuera ensuite et vous ne verrez que rarement la fenêtre de contrôle d'application, à moins que vous n'installiez un nouveau logiciel ou qu'une application malveillante tente de se connecter à Internet à partir de votre ordinateur.

Exemple : Lancement du navigateur Internet pour la première fois après l'installation

1. Lancez votre navigateur Internet (p. ex. Internet Explorer, Netscape).

2. La fenêtre de contrôle d'application apparaît, vous demandant si la tentative de connexion "Internet Explorer" doit être autorisée ou refusée.
   a. Sélectionnez *Mémoriser cette connexion pour utilisation ultérieure*, car vous savez que votre navigateur Internet est une application sûre.
   b. Cliquez sur **Autoriser**, car vous savez que le navigateur que vous avez lancé vous-même est sûr (pour en savoir plus sur ce qui peut être considéré comme sûr ou non, voir *«Utilisation du contrôle d'application »* page 70).

Vous pouvez cliquer sur **Aide** pour en savoir plus sur le contrôle d'application.

Remarque : Si vous souhaitez désactiver le contrôle d'application, accédez à la page Internet Shield. Face à Contrôle d'application, cliquez sur **Changer**. Le message d'état changera de *Invite* en *Autoriser et connecter*.

Pour plus d'informations sur le contrôle d'application, voir *«Utilisation du contrôle d'application »* page 70.

2.3 F-Secure Internet Security 2003 est-il actif et fonctionne-t-il correctement ?

Après avoir installé F-Secure Internet Security 2003 ou chaque fois que vous l'utilisez, vous pouvez vérifier que F-Secure Internet Security 2003 est actif et fonctionne correctement d'après l'icône affichée dans la barre d'état de Windows (angle inférieur droit de l'écran) comme illustré ci-dessous

Remarque : Sous Windows XP, les icônes peuvent être masquées. Pour afficher les icônes masquées, cliquez sur le bouton .

L'icône peut se présenter différemment ou non, selon l'état de F-Secure Internet Security 2003. Référez-vous à la liste des icônes ci-dessous pour connaître leur signification :

Icône	Signification	Que faire
	F-Secure Internet Security 2003 fonctionne correctement. Votre ordinateur est protégé.	Utilisez normalement votre courrier électronique et votre navigateur Internet.
	Installation en cours. Votre ordinateur n'est pas encore protégé.	Attendez la fin de l'installation. L'icône apparaît lorsque l'installation est terminée.

Icône	Signification	Que faire
	Erreur. Une erreur s'est produite dans F-Secure Internet Security 2003.	Placez le pointeur de la souris sur l'icône  pour voir la raison de l'erreur. Au besoin, faites redémarrer l'ordinateur.
	Avertissement. Une fonction de protection a été désactivée ou vos définitions de virus ne sont plus à jour. Votre ordinateur n'est pas entièrement protégé.	Placez le pointeur de la souris sur l'icône  pour voir la bulle d'aide de l'icône d'état. Activez la fonction qui est actuellement désactivée ou accédez à F-Secure Internet Security 2003 et vérifier les mises à jour.
	Déchargé. F-Secure Internet Security 2003 est désactivé et votre ordinateur n'est pas protégé.	Cliquez avec le bouton droit sur l'icône  et sélectionnez Recharger pour activer F-Secure Internet Security 2003.
Pas d'icône	F-Secure Internet Security 2003 n'est pas installé. Votre ordinateur n'est pas protégé.	Faites redémarrer l'ordinateur et installez F-Secure Internet Security 2003.

2.4 Options d'accès à F-Secure Internet Security 2003

Il existe plusieurs façons d'accéder à F-Secure Internet Security 2003 et de l'utiliser :

- Menu Démarrer de Windows
-  Icône
- Menu contextuel de F-Secure Internet Security 2003

Menu Démarrer de Windows

Pour ouvrir F-Secure Internet Security 2003, accéder aux opérations de base, voir les manuels et les pages web :

1. Ouvrez le menu *Démarrer* de Windows.
2. Pointez *Programmes* et le sous-menu F-Secure Internet Security 2003.
3. Cliquez sur Ouvrir F-Secure Internet Security 2003 pour commencer à utiliser F-Secure Internet Security 2003 ou sélectionnez une autre option dans le sous-menu de F-Secure Internet Security 2003.

Icône

Vous pouvez utiliser l'icône dans la barre d'état de Windows (angle inférieur droit de l'écran) pour ouvrir F-Secure Internet Security 2003, voir l'état du programme ou accéder à son menu contextuel.

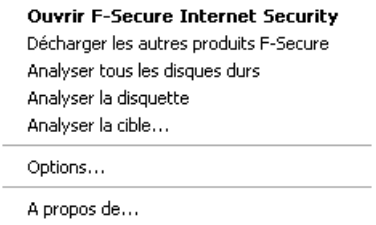
Pour ouvrir F-Secure Internet Security 2003, cliquez deux fois sur l'icône avec le bouton gauche de la souris.

Bulle d'aide de l'icône d'état F-Secure Internet Security 2003

Placez le pointeur de la souris sur l'icône pour voir la bulle d'aide de l'icône d'état F-Secure Internet Security 2003. Cette bulle d'aide permet de voir instantanément si F-Secure Internet Security 2003 a un problème, comme dans l'exemple ci-dessous où Virus Protection a été désactivé.

Menu contextuel de F-Secure Internet Security 2003

Cliquez sur l'icône avec le bouton droit de la souris pour accéder au menu contextuel F-Secure Internet Security 2003, qui contient une liste des commandes les plus utilisées. À partir de ce menu, vous pouvez ouvrir F-Secure Internet Security 2003 ou lancer immédiatement une détection de virus.



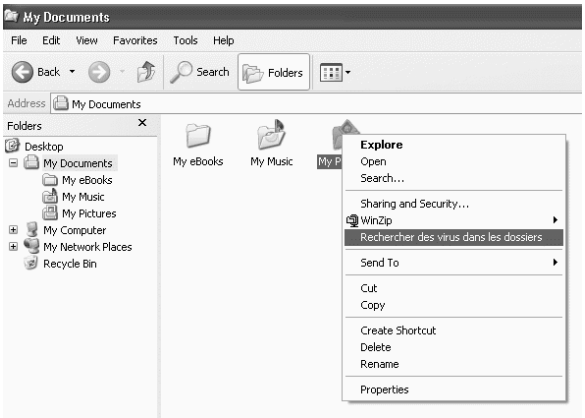
Pour mieux comprendre chaque option du menu, consulter le tableau ci-dessous :

Sélection	Explication
Ouvrir F-Secure Internet Security 2003	Ouvre F-Secure Internet Security 2003.
Décharger les autres produits F-Secure	Décharge les produits de la mémoire. Cette opération est parfois nécessaire pour l'installation de certains logiciels ou pour effectuer des tâches pour lesquelles les performances sont critiques. Ne laissez pas inutilement votre ordinateur dans cet état, car il n'est pas protégé.
Analyser tous les disques durs	Virus Protection analyse tous les disques durs disponibles sur votre ordinateur.
Analyser la disquette	Virus Protection analyse toute disquette présente dans le lecteur A:.
Analyser la cible...	Virus Protection analyse la cible de votre choix. L'arborescence des répertoires apparaît. Sélectionnez le répertoire cible et cliquez sur OK pour commencer l'analyse.
Options…	Ouvre les options avancées
A propos de...	Affiche des informations concernant F-Secure Internet Security 2003.

Menu contextuel de F-Secure Internet Security 2003

Vous pouvez analyser des disques, dossiers et fichiers à la recherche de virus avec Windows Explorer. Pour ce faire :

1. Placez le pointeur de la souris sur le disque, dossier ou fichier à analyser et cliquez avec le bouton droit de la souris.
2. Dans le menu contextuel, sélectionnez Rechercher des virus dans les dossiers. La fenêtre *Analyse manuelle* apparaît et l'analyse commence.



Si un virus est détecté, voir *«Suppression d'un virus de votre ordinateur »* page 63.

Remarque : Lorsque vous effectuez une analyse, F-Secure Internet Security 2003 utilise les paramètres d'analyse définis dans votre profil de Virus Protection actuel. Voir *«Modification du profil de protection antivirus »* page 62.

3. Accueil

La page *Accueil* présente un aperçu rapide et détaillé des paramètres de sécurité et de l'état de F-Secure Internet Security 2003.

Sur la page Accueil, vous pouvez :

- Sélectionner votre profil Virus Protection et surveiller l'état de la protection antivirus. Pour plus d'informations et des instructions, voir **Chapitre 4.** *Protection antivirus*.
- Sélectionner votre profil Internet Shield. Pour plus d'informations et des instructions, voir **Chapitre 5.** *Protection Internet*.
- Activer et désactiver les mises à jour automatiques et afficher des informations sur les mises à jour reçues sur votre ordinateur. Pour plus d'informations et des instructions, voir **Chapitre 6.** *Mises à jour automatiques*.

4. Protection antivirus

Sur la page Protection antivirus, vous pouvez :

- Sélectionner votre profil de Protection antivirus (pour plus d'informations, voir *«Profil de protection antivirus »* page 61).
- Voir quand vous avez reçu des mises à jour des définitions de virus et quand vos fichiers de définitions de virus ont été créés chez F-Secure VirusLab.
- Voir le nombre de fichiers analysés par F-Secure Internet Security 2003 et combien de virus ont été supprimés.
- Analyser manuellement des fichiers (pour plus d'informations, voir *«Rechercher des virus »* page 62).

4.1 Profil de protection antivirus

Les profils de protection antivirus permettent de changer instantanément votre niveau de protection en fonction de vos besoins. Les profils sont automatiquement mis à jour pour garantir votre protection contre les formes les plus récentes de programmes malveillants et d'attaques via Internet.

Si vous changez les paramètres d'un profil (dans la fenêtre Paramètres avancés de Protection antivirus), son nom sera changé en Personnalisé. Pour restaurer votre profil de protection antivirus, voir *Modification du profil de protection antivirus* ci-dessous.

Modification du profil de protection antivirus

Vous pouvez changer de profil à tout moment selon la protection dont vous avez besoin. Un changement de profil modifie le niveau des actions automatisées et des rapports.

Pour changer votre profil, dans la section protection antivirus :

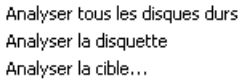
1. Cliquez sur **Modifier**.
2. Sélectionnez un profil dans la liste déroulante. Lisez attentivement la description de chaque profil avant de l'activer.
3. Cliquez sur **OK** pour utiliser le profil sélectionné.

4.2 Rechercher des virus

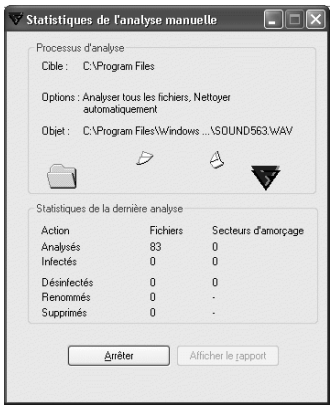
Lorsque la protection antivirus est activée, votre ordinateur est protégé. L'ouverture ou la fermeture d'un fichier entraîne automatiquement la recherche de virus dans ce fichier.

Si vous suspectez un certain fichier de contenir un virus, vous pouvez l'analyser ou analyser votre ordinateur à la recherche de virus. Pour effectuer une analyse vous-même, procédez comme suit :

1. Cliquez sur **Rechercher des virus**
2. Dans le menu, choisissez d'analyser tous les disques durs locaux, une disquette ou un dossier que vous spécifiez.



3. La fenêtre *Statistiques de l'analyse manuelle* apparaît, affichant les statistiques de l'analyse. Cliquez sur **Arrêter** pour interrompre l'analyse à tout moment.



4. A la fin de l'analyse, un rapport est généré. Cliquez sur Afficher le rapport pour visualiser le rapport dans votre navigateur Web. Si un virus est détecté, voir *«Suppression d'un virus de votre ordinateur »* page 63.

Remarque : Lorsque vous effectuez une analyse, F-Secure Internet Security 2003 utilise les paramètres définis dans votre profil de protection antivirus actuel. Pour sélectionner un autre profil, voir *«Profil de protection antivirus »* page 61.

4.3 Suppression d'un virus de votre ordinateur

Comment l'Assistant de nettoyage de F-Secure Anti-Virus supprime un virus

L'Assistant de nettoyage de F-Secure Anti-Virus apparaît si :

- un virus a été détecté lors d'une analyse ;
- un virus a été détecté et votre profil de protection antivirus est réglé pour afficher toutes les anomalies découvertes et vous les signaler avant la désinfection ;
- un virus a été détecté durant une analyse automatisée (option Protection automatique activée) et F-Secure Internet Security 2003 n'a pas pu supprimer le virus lui-même.

L'Assistant vous aide à éradiquer le virus en plusieurs étapes, comme suit.

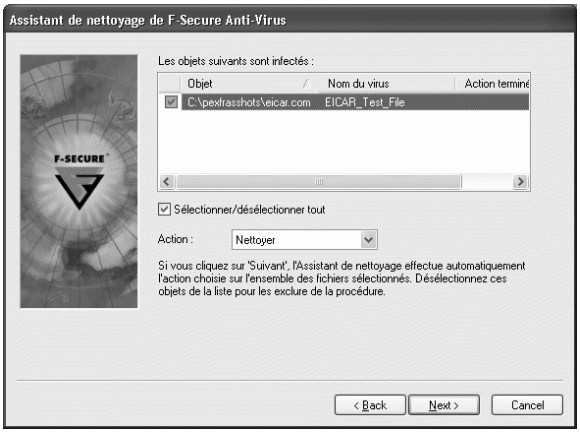
Étape 1 - Virus détecté

Le nom du virus détecté est affiché, comme illustré ci-dessous. Pour poursuivre la désinfection, cliquez sur **Suivant**.

Remarque : Pour plus d'informations sur le virus, cliquez sur son nom, puis sur Infos sur les virus. Si le virus est récent, il n'est peut-être pas décrit. Consultez le Centre d'information F-Secure sur les virus informatiques http://www.f-secure.com/v-descs/ pour obtenir les informations les plus récentes.

Étape 2 - Action exécutée

La liste des fichiers infectés s'affiche.



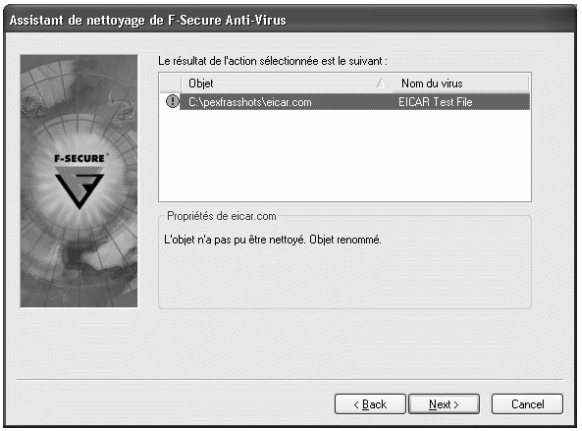
Dans la zone Action, sélectionnez l'opération à exécuter sur les fichiers infectés. Ces actions sont brièvement décrites dans le tableau ci-dessous.

Action	Explication
Nettoyer	L'Assistant de nettoyage désinfecte le fichier. **Remarque :** Si l'Assistant de nettoyage ne parvient pas à désinfecter le fichier, il tente de le renommer automatiquement.
Supprimer	L'Assistant de nettoyage supprime le fichier qui contient le virus. Toutes les informations contenues dans le fichier sont perdues. **Avertissement :** Si vous sélectionnez Supprimer, l'objet infecté est également supprimé.
Renommer	L'Assistant de nettoyage renomme le fichier de sorte qu'il ne soit pas possible de l'exécuter automatiquement. Cela empêche l'activation du virus.

Une fois que vous avez sélectionné l'action à effectuer, cliquez sur Suivant et l'Assistant de nettoyage applique automatiquement l'action choisie à tous les objets sélectionnés.

Étape 3 - Résultats de l'action

Les résultats de l'action s'affichent. Si vous avez choisi une action qui a échoué, vous pouvez revenir en arrière et répéter l'étape 2 pour choisir une autre action.



Si le nettoyage et la suppression échouent, vous pourrez éventuellement choisir de renommer le fichier. C'est généralement une bonne option pour les exécutables (.exe) infectés, car elle change l'extension en une extension de fichier qui n'est pas autorisée à s'exécuter automatiquement.

Notez que, si le nettoyage a échoué, il se peut que l'Assistant de nettoyage l'ait déjà automatiquement renommé (voir le tableau des actions ci-dessus). Dans ce cas, une note à cet effet apparaît dans le champ *Propriétés*.

Remarque : Si un nouveau virus est découvert, si les définitions de virus ne sont plus à jour ou si vous recevez une fausse alerte, le nettoyage ou la suppression peuvent échouer. Pour des instructions sur ce qu'il faut faire dans ce cas, voir *«Suppression d'un virus lorsque l'Assistant de nettoyage échoue »* page 66.

Si l'opération a réussi, cliquez sur **Suivant** pour continuer.

Étape 4 - Vérifier et terminer

Un rapport de nettoyage sera généré après la fin du processus de nettoyage. Si vous ne souhaitez pas obtenir de rapport, ne cochez pas la case Créer le rapport. Notez que le rapport de nettoyage n'est pas généré pour les virus trouvés lors d'une analyse automatisée.

Cliquez sur **Terminer** pour quitter l'Assistant de nettoyage.

Le rapport de nettoyage s'affiche dans le navigateur Web par défaut et contient des liens vers les descriptions de virus correspondantes dans la base de données des virus du Web Club.

Remarque : Si le virus a été détecté dans un fichier qui était verrouillé par un autre processus au moment où l'Assistant de nettoyage a tenté de le supprimer, une fenêtre apparaîtra pour demander de faire redémarrer l'ordinateur. Si cette fenêtre apparaît, enregistrez tous vos documents ouverts et suivez les instructions affichées.

Suppression d'un virus lorsque l'Assistant de nettoyage échoue

Si l'Assistant de nettoyage n'a pas pu nettoyer ou supprimer le fichier, une des conditions suivantes est probablement à l'origine de cet échec :

- La base de données des définitions de virus n'est plus à jour. Vérifiez que vous possédez les fichiers de définition les plus récents et réessayez (voir **Chapitre 6.** *Mises à jour automatiques*.)
- Fausse alerte. Tout est fait pour que F-Secure Internet Security 2003 évite de déclarer infecté un fichier inoffensif, mais la nature complexe des fichiers fait qu'un fausse suspicion est toujours possible.
- Un nettoyage manuel est nécessaire. Dans certains cas, vous devez exécuter un outil qui nettoie le fichier et supprime le virus. C'est souvent le cas pour des virus plus modernes utilisant des techniques avancées pour se cacher et s'attacher à vos fichiers.
- Vous avez découvert un nouveau virus. Un nouveau type de virus peut avoir infecté votre ordinateur. Pas de panique. Vos fichiers sont en sécurité, puisque F-Secure Internet Security 2003 a détecté et arrêté le virus avant qu'il fasse des dégâts.

Si vous êtes certain que le fichier est sans danger, vous pouvez ignorer les avertissements. Vous pouvez configurer la protection automatique et l'analyse manuelle pour qu'elles ignorent ce fichier lors de prochaines analyses. Pour ce faire, voir *«Demander à la Protection antivirus d'ignorer/ analyser certains fichiers »* page 67.

Comment supprimer manuellement le virus

1. Essayez de nettoyer le fichier vous-même. Pour supprimer plus facilement le virus, vous pouvez, au choix :
   - Consulter le Centre d'information F-Secure sur les virus informatiques http://www.f-secure.com/v-descs/ pour obtenir des informations sur le virus. Ces informations vous aideront à supprimer le virus et peuvent comprendre un lien vers l'outil nécessaire pour ce faire.
   - Utilisateurs avancés : Accédez directement à ftp://ftp.europe.f-secure.com/anti-virus/tools/ pour trouver un outil de nettoyage adapté.

   Les outils contiendront toutes les instructions à suivre pour supprimer le virus de votre système.
2. Si vous avez essayé d'utiliser l'Assistant de nettoyage sans succès, que votre base de données des définitions de virus est à jour et que les outils de nettoyage proposés sur le site Web de F-Secure n'apportent pas de solution, suivez les instructions de la section *«Que faire si vous pensez avoir trouvé un nouveau virus ? »* page 67.

4.4 Que faire si vous pensez avoir trouvé un nouveau virus ?

Si F-Secure Internet Security 2003 vous avertit que vous avez un fichier infecté par un virus, mais ne peut pas vous donner le nom du virus ni le nettoyer ou le supprimer, il se peut qu'il s'agisse d'un tout nouveau virus. Tant que vous n'avez pas la certitude que le virus potentiel a été supprimé ou qu'il s'agissait d'une fausse alerte, n'essayez pas d'utiliser le fichier.

Pour supprimer le virus, procédez comme suit :

1. Vérifiez que votre base de données de définitions de virus est à jour. Un fichier de définitions plus récent peut indiquer à F-Secure Internet Security 2003 comment traiter le virus et le supprimer de votre ordinateur.
2. Si vous avez déjà les définitions de virus les plus récentes (voir **Chapitre 6.** *Mises à jour automatiques*.), vérifiez sur le site de F-Secure s'il existe des outils que vous pouvez utiliser pour supprimer manuellement le virus (http://www.f-secure.com/v-descs/ ou ftp://ftp.europe.f-secure.com/anti-virus/tools/).
3. Si ces mesures échouent, envoyez le fichier à F-Secure VirusLab. Pour des instructions, visitez :

   http://www.f-secure.com/support/technical/general/samples.shtml.

4.5 Demander à la Protection antivirus d'ignorer/analyser certains fichiers

Dans certains cas, vous souhaiterez demander à la Protection d'ignorer certains types de fichiers ou des fichiers spécifiques. Par exemple :

- Vous êtes certain qu'un fichier n'est pas infecté, mais recevez des fausses alertes.

- Votre ordinateur possède des ressources limitées et l'analyse de tous les fichiers par Virus Protection ralentirait l'ordinateur de manière insupportable.
- Le fichier est d'un type qui n'est jamais infecté par un virus.

Certains profils règlent déjà l'analyse automatisée de manière à analyser certains types de fichiers. Ces réglages offtrent un bon équilibre entre la nécessité d'analyser les fichiers contenant généralement des virus et la limitation de l'impact sur le temps processeur et la mémoire.

Avertissement : Si vous demandez à la Protection d'ignorer certains fichiers, ces fichiers restent exposés à une attaque virale furure et cela limite la possibilité de détecter et de nettoyer des virus. Cet usage n'est donc recommandé que dans des cas extrêmes.

Réglage de la protection en temps réel ou de l'analyse manuelle pour analyser certains fichiers

Pour demander à la protection en temps réel ou à l'analyse manuelle d'analyser certains fichiers :

1. Ouvrez la fenêtre principale de F-Secure Internet Security 2003.
2. Sélectionnez la page Protection antivirus et cliquez sur Paramètres avancés. Dans les onglets Protection en temps réel et Analyse manuelle, assurez-vous que l'option Fichiers avec ces extensions est cochée.

Réglage de la protection en temps réel ou de l'analyse manuelle pour ignorer certains fichiers

Pour demander à la protection en temps réel ou à l'analyse manuelle d'ignorer certains fichiers :

1. Ouvrez la fenêtre principale de F-Secure Internet Security 2003.
2. Sélectionnez la page Protection antivirus et cliquez sur **Paramètres avancés.** Dans les onglets Protection en temps réel et Analyse manuelle, assurez-vous que :
   - l'option Exclure les fichiers avec ces extensions est cochée, puis entrez les extensions de fichiers dans la zone de texte.
   - l'option Exclure les objets (fichiers, dossiers...) est cochée. Cliquez sur **Sélectionner** pour parcourir les fichiers à exclure et les ajouter à la liste des fichiers à exclure.

5. Protection Internet

Sur la page Protection Internet, vous pouvez :

- Sélectionner votre profil de Protection Internet (pour plus d'informations, voir *«Profils de Protection Internet »* page 70).
- Changer l'état du contrôle d'application. Pour ce faire, cliquez sur **Modifier** face à l'état actuel du contrôle d'application.
- Vérifier combien d'applications sont autorisées à se connecter à Internet. Pour changer les droits de connexion d'une application, voir *«Modification des droits de connexion d'une application »* page 70.
- Changer votre configuration d'alerte. Pour ce faire, cliquez sur **Modifier** face à l'état actuel.
- Voir combien d'alertes vous avez reçues depuis la date spécifiée. Cliquez sur **Afficher** pour voir une liste des alertes.
- Vérifier combien de paquets ont été éliminés. Les paquets dangereux connus sont toujours éliminés par Internet Shield, mais vous pouvez aussi affecter cette fonction en personnalisant les règles d'Internet Shield (voir *«Personnalisation des profils de Protection Internet »* page 72).
- Vérifier quand vous avez reçu la dernière alerte Internet Shield. Cliquez sur **Détails** pour afficher les détails de la dernière alerte et les cinq protocoles et hôtes (adresses IP) les plus fréquemment bloqués.

5.1 Profils de Protection Internet

Les profils de Protection Internet permettent de changer instantanément le niveau de protection en fonction de vos besoins ; ils sont automatiquement mis à jour afin de garantir votre protection contre les formes les plus récentes des programmes malveillants et attaques Internet.

Modification du profil de Protection Internet

Vous pouvez changer de profil à tout moment selon la protection dont vous avez besoin. Un changement de profil modifie le niveau des actions automatisées et des rapports.

Pour changer votre profil, dans la section Protection Internet :

1. Cliquez sur **Modifier**.
2. Sélectionnez un profil dans la liste déroulante. Lisez la description de chaque profil avant de l'activer.
3. Cliquez sur **OK** pour utiliser le profil sélectionné.

Pour personnaliser un profil, voir *«Personnalisation des profils de Protection Internet »* page 72.

5.2 Utilisation du contrôle d'application

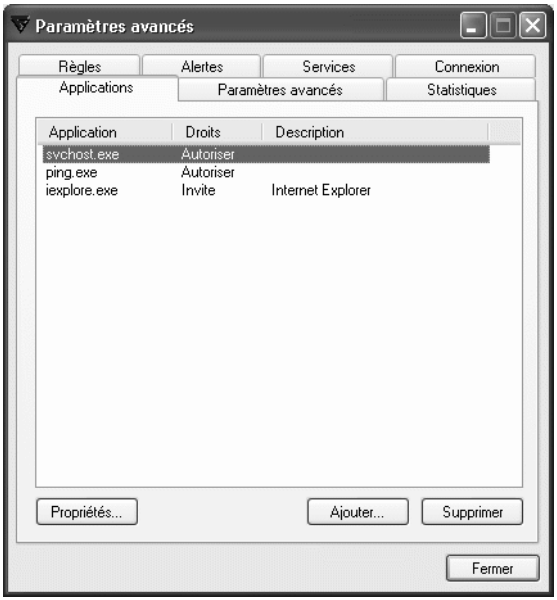
Le contrôle d'application est une fonction de F-Secure Internet Security 2003 qui vérifie toutes les applications se connectant à Internet à partir de votre ordinateur. Le contrôle d'application vous demande si la tentative de connexion de l'application doit être autorisée ou refusée, comme décrit sous *«Que faire lorsque la fenêtre de contrôle d'application apparaît ? »* page 53. Autorisez les applications connues et sûres à se connecter à Internet ; si une application n'est pas sûre, refusez-lui de se connecter.

Un fichier intitulé Journal des actions enregistre toutes les connexions et leurs propriétés pour vous permettre de voir où votre ordinateur s'est connecté. Pour y accéder, cliquez sur **Paramètres avancés**, puis sur l'onglet *Connexion*.

Modification des droits de connexion d'une application

Si vous souhaitez changer les droits de connexion ou les propriétés d'une application, procédez comme suit :

1. Accédez à la page Protection Internet et cliquez sur **Modifier** face à *Applications autorisées/ refusées*.
2. La page *Paramètres de Protection Internet* s'ouvre.



3. Sélectionnez l'application dont vous souhaitez changer les propriétés (les droits actuels sont indiqués dans la colonne Droits). Cliquez sur **Propriétés**.
4. Sélectionnez Refuser, Invite ou Autoriser. Cliquez sur **OK** pour retourner à la page Applications.
5. Les nouveaux droits de l'application apparaissent dans la colonne Droits face au nom de l'application. Cliquez sur **Fermer** pour terminer.

Quels sont les éléments pouvant être considérés comme "fiables" ?

- Une application connue que vous avez lancée vous-même.
- Des services Windows se connectant à Internet.

Des services Microsoft Windows sûrs

Certains services Microsoft Windows exigent un accès au réseau pour fonctionner. La plupart des services sont automatiquement autorisés mais le contrôle d'application peut vous demander d'autoriser ou non les services ci-dessous, en particulier sur les plates-formes Windows NT 4.0, Windows 2000 et Windows XP. Autorisez ces services à accéder au réseau, faute de quoi certaines fonctionnalités Windows risquent de ne pas marcher.

Liste des applications :

Remarque : %Winnt% se réfère au répertoire d'installation de Windows, généralement C:\Winnt\

Exécutable	Emplacement	Description	Trafic réseau
SVCHOST.EXE	%Winnt%\System32\	Processus hôte générique pour les services Win32	udp/67 out, udp/68 in, udp/137 out
SPOOLSV.EXE	%Winnt%\System32\	Sous-système de spoule	udp/137 out, udp/ 138 out
LSASS.EXE	%\Windows%\System32\	Exécutable LSA et DLL Serveur	udp/137 out
SERVICES.EXE	%Winnt%\System32\	Application Services et Contrôleur	udp/67 out, udp/68 in, udp/137 out
WINLOGON.EXE			udp/137 out

Quels sont les éléments pouvant être considérés comme "non fiables" ?

Les applications reçues d'une source non fiable doivent toujours être traitées comme suspectes. Les applications reçues d'une source fiable sans accord préalable doivent toujours être traitées comme suspectes.

- Toute application que vous n'avez pas installée vous-même ou que vous ne connaissez pas.
- Toute application considérée comme fiable, mais qui tente de se connecter sans que vous l'ayez lancée.
- Toute connexion ne contenant pas de nom cible (adresse Web sous forme de texte) propre.

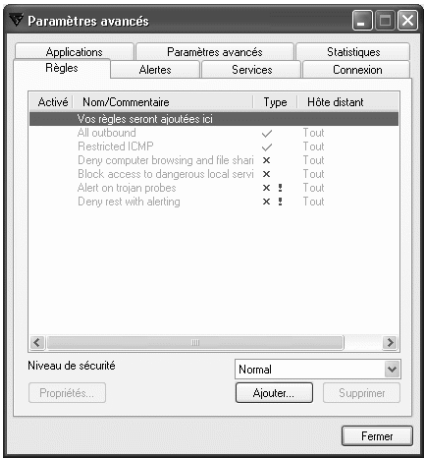
5.3 Personnalisation des profils de Protection Internet

Dans certains cas, vous souhaiterez ajouter, modifier ou supprimer les règles définissant que faire de certaines connexions. Ces situations se produisent lorsque vous souhaitez :

- Vous connecter à un nouveau serveur de jeux sur un ordinateur particulier.
- Autoriser les connexions en général, mais bloquer une connexion à un site ou à un ordinateur particulier que vous ne considérez pas comme fiable.

Pour personnaliser vos paramètres de Protection Internet :

1. Cliquez sur **Paramètres avancés** sur la page Protection Internet. La fenêtre Paramètres avancés s'ouvre.
2. Dans le menu déroulant Niveau de sécurité, sélectionnez le profil à personnaliser.
3. Cliquez sur l'onglet Règles (s'il n'est pas encore sélectionné).



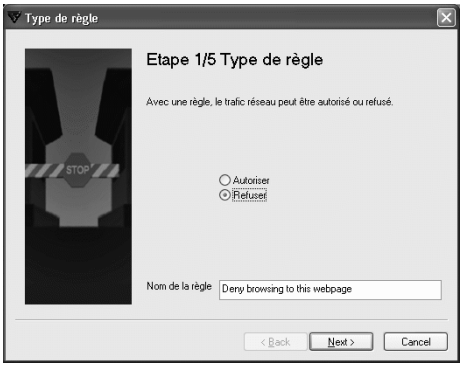
- Pour modifier une règle existante, sélectionnez-la dans la liste et cliquez sur **Propriétés**.
- Pour ajouter une règle, cliquez sur **Ajouter**.
- Pour supprimer une règle, sélectionnez-la dans la liste et cliquez sur **Supprimer**.

Remarque : Il n'est pas possible de modifier ni de supprimer les règles prédéfinies. Vous pouvez uniquement ajouter des règles ou changer/supprimer des règles que vous avez créées vous-même.

Création d'une nouvelle règle de protection Internet

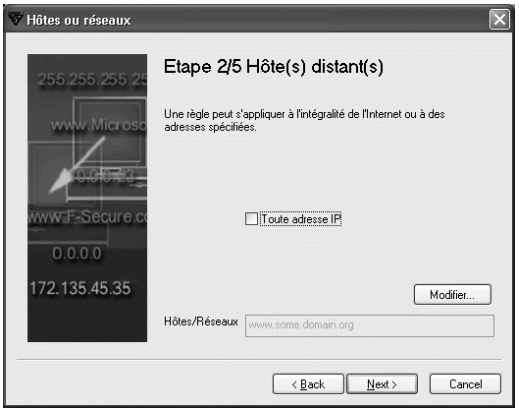
Étape 1 – Type de règle

Donnez un nom descriptif à la règle et choisissez d'autoriser ou refuser la connexion.



Étape 2 - Spécifiez la (les) cible(s)

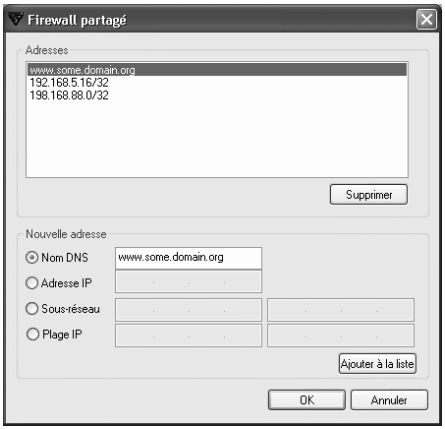
Choisissez si cette règle s'applique à toutes les connexions en cours ou à certaines connexions uniquement.



Vous pouvez :

- Cocher Toute adresse IP pour appliquer la règle à toutes les connexions Internet et cliquer sur **Suivant** pour passer à l'étape 3 ou
- Désélectionner Toute adresse IP et cliquer sur **Modifier** pour ouvrir une nouvelle fenêtre où vous pouvez entrer les détails des cibles.
- Les cibles peuvent être énumérées dans un ordre quelconque et peuvent être n'importe quel nom DNS, adresse IP, sous-réseau (au format de masque de réseau binaire) ou plage d'adresses IP. Par exemple :

Nom DNS :	www.un.domaine.org
Adresse IP :	192.168.5.16
Sous-réseau :	192.168.88.0/29
Plage IP :	192.168.1.1-192.168.1.63

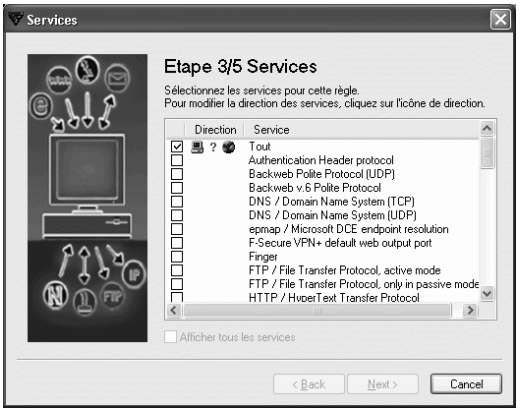


Cliquez sur **Ajouter à la liste** pour ajouter la nouvelle cible à la liste de cibles auxquelles s'applique la règle. Pour supprimer une adresse cible, sélectionnez-la dans la liste et cliquez sur **Supprimer**. Pour modifier les propriétés d'une cible, sélectionnez-la dans la liste. Cliquez sur **OK** pour retourner à la page Hôte(s) distant(s) et cliquez sur **Suivant** pour continuer.

Étape 3 - Choisissez le service et la direction de la règle

Dans la liste des services disponibles, choisissez le service auquel cette règle s'appliquera. Si vous voulez que la règle s'applique à tous les services, sélectionnez *Tous* dans le haut de la liste.

Vous pouvez sélectionner autant de services individuels que vous le souhaitez.

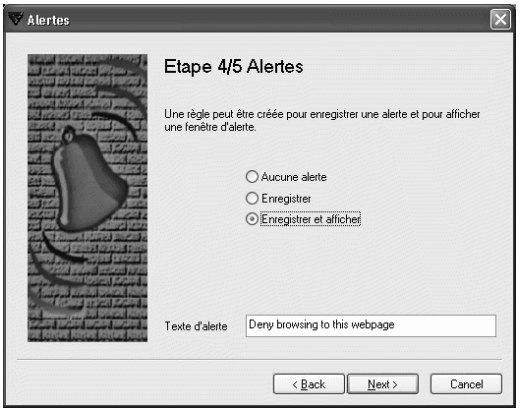


Pour les services choisis, sélectionnez la direction dans laquelle s'applique la règle en cliquant sur le point d'interrogation rouge qui apparaît. Continuez à cliquer pour faire défiler les options disponibles en boucle. Pour des exemples, consultez le tableau ci-dessous.

Sélection	Terme	Explication
	Non défini	La direction n'a pas encore été définie. Cliquez sur le graphique pour définir une direction.
	Entrant	Le service sera autorisé /refusé s'il provient d'Internet en direction de votre ordinateur.
	Sortant	Le service sera autorisé /refusé s'il provient de votre ordinateur en direction d'Internet.
	Les deux	Le service sera autorisé /refusé dans les deux directions, qu'il provienne de votre ordinateur ou s'y dirige.

Étape 4 - Choisissez la connexion et l'option de création de rapports

Vous pouvez choisir d'être informé ou non chaque fois que la règle est appliquée à une tentative de connexion.



- *Aucune alerte* : vous ne recevrez aucune information lorsque la règle est appliquée à une connexion.
- *Enregistrer* : des données concernant la connexion sont enregistrées dans un fichier.
- *Enregistrer et afficher* : des données sont enregistrées et une fenêtre de notification s'affiche par exemple lorsque la connexion est autorisée/refusée.

Étape 5 - Vérifier et accepter la règle

Vous pouvez maintenant vérifier la règle. Cliquez sur **Précédente** pour revoir la règle et apporter des modifications éventuelles.

Si vous êtes satisfait de votre nouvelle règle, cliquez sur **Terminer**. Votre nouvelle règle sera ajoutée en haut de la liste des règles actives sur l'onglet Règles des paramètres Internet Shield.

5.4 Paramètres avancés

Remarque : Cette section concerne uniquement les utilisateurs avertis. La modification des réglages peut désactiver Internet Shield.

Pour accéder aux paramètres avancés de Protection Internet, cliquez sur **Paramètres avancés** dans la page Protection Internet. Cliquez sur l'onglet Avancé dans la fenêtre qui apparaît.

Les éléments suivants doivent être pris en considération lors de la personnalisation des paramètres avancés de la protection Internet.

Interface fiable

Cette option peut être utilisée si l'ordinateur où est installé F-Secure Internet Security 2003 sert de passerelle réseau, p. ex. si le partage de connexion Internet est activé dans Windows. L'interface réseau utilisée pour le réseau local peut être réglée sur « Interface fiable » de sorte qu'aucune règle de protection Internet ne s'y applique.

Remarque : Cette interface réseau sera laissée complètement ouverte et n'est pas protégée.

Filtre de paquets

Le filtrage de paquets est la fonction principale du module de protection Internet Shield ; si vous le désactivez, Internet Shield sera grandement inefficace contre tous les types d'attaques réseau.

Contrôle d'application

Ne désactivez pas le contrôle d'application dans la fenêtre Paramètres avancés. La désactivation du contrôle d'application augmente le risque d'attaques basées sur un logiciel et ne doit se faire qu'à des fins de dépannage, etc.

Si vous souhaitez désactiver le contrôle d'application, accédez à la page Protection Internet et changez l'état du contrôle d'application de *Invite* en *Autoriser et connecter*.

6. Mises à jour automatiques

Le service de mise à jour automatique s'active de manière transparente à l'arrière-plan chaque fois que vous vous connectez à Internet et veille à ce que vous receviez les mises à jour les plus récentes sur votre ordinateur.

Dans la section Mises à jour automatiques, vous pouvez :

- Cliquer sur **Activer** ou **Désactiver** les mises à jour automatiques.
- Voir quand a eu lieu le dernier contrôle de mise à jour et/ou quand aura lieu le prochain.

  Si vous souhaitez vérifier personnellement que vous possédez les définitions de virus les plus récentes, cliquez sur **Vérifier maintenant**. Si vos définitions ne sont pas à jour, les versions les plus récentes sont alors téléchargées.

Remarque : Si vous utilisez un modem ou une liaison RNIS pour vous connecter à Internet, cette connexion doit être active pour que le contrôle de mise à jour puisse avoir lieu.

Remarque pour les utilisateurs de lignes RNIS : Par défaut, les mises à jour automatiques sont programmées une fois par heure. Cela signifie qu'une connexion à Internet sera ouverte une fois par heure si vous avez un routeur RNIS ou un système similaire de numérotation automatique (et chaque connexion vous coûtera de l'argent). Si vous souhaitez empêcher votre routeur RNIS d'établir automatiquement la connexion, désactivez la fonction Mises à jour automatiques et utilisez le bouton **Vérifier maintenant** pour vérifier les mises à jour.

- Vérifiez la dernière mise à jour des trois éléments ci-dessous.

Définitions de virus	Base de données de protection antivirus, fréquemment mise à jour. Ces mises à jour automatiques sont effectuées de manière transparente à l'arrière-plan, sans intervention de votre part, et s'activent chaque fois que vous vous connectez à Internet.
Profils de sécurité	Divers niveaux de paramètres de sécurité. Pour une protection maximale de votre ordinateur, les profils sont mis à jour chaque fois que de nouveaux types d'attaques sont découverts.
Logiciel	Les mises à jour du logiciel F-Secure Internet Security 2003 sont téléchargées à l'arrière-plan.

7. Mon abonnement

La page Mon abonnement affiche des informations concernant votre abonnement personnel.

Sur cette page, vous pouvez :

- Consulter l'état de votre abonnement. La date d'échéance de votre abonnement est indiquée, ainsi que l'état actuel et une des icônes d'état suivantes :

	Valide	Votre abonnement est valide.
	Bientôt à expiration	Votre abonnement est valide mais vient bientôt à expiration.
	Expiré	Votre abonnement a expiré.

- Renouveler votre abonnement en ligne (ou, si vous utilisez une version d'évaluation, vous pouvez acheter un nouvel abonnement).
- Changer votre numéro d'abonnement.

8. Comment F-Secure Internet Security 2003 protège votre ordinateur

8.1 Protection antivirus

On appelle "antiprogrammes" diverses formes de programmes ou fichiers tels que virus, vers, chevaux de Troie, blagues et canulars développés dans le but de nuire à votre ordinateur.

Virus Protection détecte et supprime les virus et autres programmes informatiques malveillants de votre ordinateur. Chaque fois qu'il y a accès à un fichier, que ce soit à partir du disque dur de votre propre ordinateur, d'une unité de stockage externe ou d'Internet, la fonction Virus Protection de F-Secure Internet Security 2003 vérifie que le fichier ne contient pas de virus.

Un logiciel de protection antivirus combiné au chargement automatique des définitions virus les plus récentes garantit la meilleure protection possible contre les virus. Le laboratoire de recherche F-Secure Anti-Virus publie et met à jour régulièrement les définitions de virus, les profils et le logiciel F-Secure Internet Security 2003, que le programme télécharge rapidement et automatiquement chaque fois que vous vous connectez à Internet.

F-Secure Virus Protection utilise plusieurs moteurs de détection de virus afin d'assurer une protection sans faille contre les virus. Parmi ceux-ci, le moteur de détection heuristique protège particulièrement contre les virus nouveaux et inconnus.

8.2 Protection Internet - Internet Shield

Chaque fois que votre ordinateur est connecté à Internet, il constitue une cible pour les attaques de sources inconnues à travers le réseau Internet. Dans certains cas, ces attaques ne sont pas agressives, mais sont des messages inoffensifs parvenus à votre ordinateur par accident. Dans d'autres cas, en revanche, une personne ou un ordinateur inconnu tente délibérément d'accéder à votre ordinateur et à vos fichiers.

La sécurité de votre ordinateur peut être compromise de diverses manières, notamment :

- Des services laissés ouverts par inadvertance peuvent facilement être trouvés et utilisés à mauvais escient par des personnes extérieures.

Internet Shield protège votre ordinateur pendant que vous êtes connecté à Internet. Cette fonction n'autorise que les connexions de/vers votre ordinateur définies dans votre profil sélectionné. Tout autre traffic est rejeté, ce qui réduit sensiblement les possibilités pour l'intrus de visualiser/modifier les informations sur votre ordinateur.

- Votre ordinateur diffuse des informations le concernant. Lorsqu'il est connecté à Internet, quiconque sait comment lire ces informations peut les utiliser pour déployer une attaque contre vous.

Internet Shield empêche votre ordinateur de diffuser sur Internet des informations sur lui-même et bloque toute connexion sortante qui tente de laisser filtrer des informations vous concernant ou concernant votre ordinateur.

- Certains chevaux de Troie se cachent à l'intérieur de logiciels qui sont normalement fiables. Ils utilisent une connexion ou une application que vous croyez sûre pour transférer des données à votre sujet ou celui de votre ordinateur.

Internet Shield identifie les tentatives de chevaux de Troie de transférer des données et empêche la connexion, protégeant ainsi vos données en permanence contre les attaques.

8.3 Comment se prémunir contre les virus et autres antiprogrammes

F-Secure Internet Security 2003 constitue la meilleure ligne de défense contre les virus en bloquant les virus connus avant qu'ils infestent votre ordinateur. Cependant, vous pouvez aussi contribuer à la protection de votre ordinateur :

- Tenez à jour votre système d'exploitation et vos applications et appliquez les correctifs les plus récents dès qu'ils sont disponibles. Procurez-vous les mises à jour directement auprès du fournisseur.
- Lorsque vous téléchargez des fichiers, enregistrez-les toujours sur votre disque dur avant de les ouvrir ou de les exécuter. En enregistrant un fichier téléchargé, vous permettez à F-Secure Internet Security 2003 de le vérifier.
- La plupart des vers utilisent des messages électroniques pour se diffuser et visent les utilisateurs de Microsoft Outlook ou Outlook Express. Si vous devez utiliser une version d'Outlook, cherchez, téléchargez et installez régulièrement les correctifs de sécurité Outlook publiés par Microsoft.

- Lorsque vous recevez par courrier électronique des annonces non sollicitées ou si un message reçu d'un ami vous paraît bizarre, n'ouvrez pas les pièces jointes et ne cliquez pas sur les liens contenus dans le message. Si vous souhaitez voir le contenu d'une pièce jointe, enregistrez-le sur votre disque dur avant de l'ouvrir. F-Secure Internet Security 2003 peut ainsi vérifier si la pièce jointe ne contient pas de virus.
- Évitez les fichiers provenant de groupes de news publics et de systèmes de conversation en ligne tels qu'IRC et ICQ.
- Évitez de transférer les annonces de virus ou messages en chaîne que vous recevez.

Dépannage

Installation

Q. Échec de l'installation. Pourquoi ?

R. S'il n'y avait pas de connexion Internet, F-Secure Internet Security 2003 n'a pas pu valider votre abonnement. Assurez-vous que vous avez une connexion Internet et réinstallez F-Secure Internet Security 2003.

Utilisation générale

Q. F-Secure Internet Security 2003 est très lent et/ou ne s'ouvre pas. Quel est le problème ?

R. Internet Explorer 3.0 (ou plus récent) n'est peut-être pas installé. Vérifiez si Internet Explorer est installé et contrôlez le numéro de version (Internet Explorer est disponible sur le site web de Microsoft Corporation).

Q. Je ne vois pas l'icône de F-Secure Internet Security 2003 dans la barre d'état du système en bas à droite de l'écran.

R. Sous Windows XP, les icônes peuvent être masquées. Pour afficher les icônes masquées, cliquez sur le bouton  . Si vous n'utilisez pas Windows XP, installez F-Secure Internet Security 2003.

 Protection antivirus

Q. F-Secure Internet Security 2003 ne peut pas désinfecter/supprimer/renommer un fichier infecté sur mon ordinateur. Que dois-je faire ?

R. Voir *«Suppression d'un virus lorsque l'Assistant de nettoyage échoue »* page 66.

Protection Internet - Internet Shield

Q. (Je pense que) je suis attaqué par un pirate via Internet. Que dois-je faire ?

R. Ouvrez la page Internet Shield et sélectionnez le profil Bloquer tout. Pour plus d'informations sur la sélection d'un profil Internet Shield, voir *«Modification du profil de Protection Internet »* page 70.

Contrôle d'application

Q. Comment puis-je changer les droits de connexion Internet de l'application ? Comment puis-je autoriser une application à se connecter à Internet si je l'ai bloquée précédemment ?

R. Voir *«Modification des droits de connexion d'une application »* page 70.

Q. Mon programme de messagerie (ou un autre programme tel que le navigateur Internet) ne fonctionne plus.

R. Vous avez peut-être accidentellement refusé au programme de se connecter. Voir *«Modification des droits de connexion d'une application »* page 70 pour des informations sur la façon d'autoriser le programme à se connecter.

Q. Quels programmes/applications puis-je autoriser à se connecter à Internet ?

R. Voir *«Utilisation du contrôle d'application »* page 70 pour vous aider à décider quelles applications autoriser (ou non) à se connecter.

Mises à jour automatiques

Q. Que se passe-t-il si mon ordinateur n'est pas connecté lorsqu'une mise à jour automatique des virus doit avoir lieu ?

R. La prochaine fois que vous êtes en ligne, F-Secure Internet Security 2003 téléchargera la mise à jour la plus récente des virus.

Q. À quelle fréquence faut-il mettre à jour les bases de données de définitions de virus ?

R. Les bases de données de définitions de virus sont automatiquement mises à jour si la fonction Mises à jour automatiques est activée. Si vous voulez mettre à jour manuellement les bases de données, faites-le au moins une fois par semaine.

Q. J'essaie de vérifier manuellement s'il y a des mises à jour des bases de données de définitions de virus (en cliquant sur Vérifier maintenant) mais rien ne se passe.

R. Si vous utilisez un modem ou avez une connexion RNIS, vous devez vous connecter manuellement à Internet avant de cliquer sur **Vérifier maintenant**.

Mon abonnement

Q. Je suis en train d'installer un logiciel, mais Virus Protection m'informe que ce logiciel contient un virus et je ne peux donc pas achever l'installation.

R. Si vous êtes sûr que le logiciel ne contient pas de virus, vous pouvez effectuer une des opérations suivantes :

- Choisissez un profil Virus Protection moins strict (pour les instructions, voir *«Modification du profil de protection antivirus »* page 62), ou
- Cliquez avec le bouton droit sur l'icône dans la barre d'état du système (en bas à droite de l'écran) et choisissez *Décharger les autres produits F-Secure*. N'oubliez pas de recharger les produits après l'installation.

Glossaire

Antiprogramme

Programmes ou fichiers développés dans le but de nuire. Cela comprend les virus informatiques, les vers et les chevaux de Troie.

Application

Programme logiciel écrit pour un usage spécifique. Généralement, les applications se lancent manuellement.

Base de données des définitions des virus

Base de données utilisée pour détecter des virus. Chaque fois qu'un nouveau virus est trouvé, la base de données doit être mise à jour afin que le module de protection puisse le détecter.

Cheval de Troie

Programme qui effectue intentionnellement une action à laquelle l'utilisateur ne s'attend pas.

Contrôle d'application

Contrôle d'application est une fonction de F-Secure Internet Security 2003 qui vérifie automatiquement si une application est autorisée à se connecter à Internet à partir de votre ordinateur en comparant l'application à une liste des logiciels sûrs (pré-approuvés) et des logiciels malveillants connus (chevaux de Troie, etc.).

DNS (système de nom de domaine)

DNS est la façon dont les noms de domaines Internet sont localisés et convertis en adresses IP (Internet Protocol). Un nom de domaine est un « pointeur » facile à retenir menant à une adresse Internet. Par exemple, l'adresse Internet www.un.domaine.org est un nom DNS.

DoS (refus de service)

Tentative explicite d'agresseurs d'empêcher les utilisateurs légitimes d'accéder à un service en rompant les connexions, en inondant un réseau ou en empêchant un individu d'accéder au réseau.

Heuristique

Méthode exploratoire de résolution de problèmes utilisant des techniques d'auto-apprentissage.

Paquet

Unité de données acheminée entre une origine et une destination sur Internet. Lorsqu'un fichier (p. ex. un message électronique) est envoyé d'un endroit à un autre sur Internet, il est divisé en paquets d'une taille appropriée pour assurer un routage efficace. Une fois tous les paquets parvenus à destination, ils sont assemblés pour reconstituer le fichier d'origine.

Profil

Attributs préconfigurés définissant votre niveau de sécurité. Les profils sont automatiquement mis à jour pour garantir votre protection contre les formes les plus récentes de programmes malveillants et d'attaques via Internet.

Sous-réseau

Section d'un réseau. Les ordinateurs situés dans le même sous-réseau sont généralement proches les uns des autres physiquement et ont des adresses IP qui commencent par les deux ou trois mêmes chiffres.

Ver

Programme capable de se répliquer par l'insertion de copies dans les ordinateurs reliés en réseau.

Virus

Programme qui se répand en se reproduisant.

Support et maintenance

L’assistance technique relative au logiciel F-Secure Internet Security 2003 est assurée par :

WSKA Editions
3 rue Joseph Cugnot
57070 Metz – France

Tél : 03.87.18.78.00
Fax : 03.87.18.78.01
E-mail : supptech@wska.com
Web : www.wska.com

F-Secure Internet Security 2003

Win 95/98/ME/NT 4.0/2000/XP

Benutzerhandbuch

Über dieses Handbuch

Dieses Handbuch enthält alle Informationen, die Sie zur Installation und Verwendung von F-Secure Internet Security 2003 benötigen.

Kapitel 1. *F-Secure Internet Security 2003 installieren*. Enthält die zur Installation von F-Secure Internet Security 2003 erforderlichen Informationen.

Kapitel 2. *Erste Schritte*. Bietet Informationen zum Zugriff auf F-Secure Internet Security 2003 sowie erste Schritte für neue Benutzer bzw. Hinweise für bereits erfahrenere Benutzer.

Kapitel 3. *Homepage*. Bietet eine detaillierte Übersicht zu Ihren Sicherheitseinstellungen und den Status von F-Secure Internet Security 2003.

Kapitel 4. *Virenschutz*. Erklärt die Aktivierung bzw. Deaktivierung des Virenschutzes, Auswahl Ihres Virenschutzprofils sowie die Überwachung nach Erhalt von Virendefinitions-Aktualisierungen.

Kapitel 5. *Internet Shield*. Erklärt das Ändern und Bearbeiten von Internet Shield-Profilen, das Überprüfen der zugelassenen und abgelehnten Verbindungen sowie den Zugriff auf erweiterte Einstellungen.

Kapitel 6. *Automatische Aktualisierungen*. Enthält Informationen zum automatischen Aktualisierungsservice, der für Sie die neuesten Vireninformationen, Software-Versionen und Profilversionen bereitstellt.

Kapitel 7. *Meine Anmeldung*. Erklärt, wie Sie Ihren Anmeldestatus anzeigen, Ihre Anmeldung verlängern sowie Ihre Anmeldenummer ändern können.

Kapitel 8. *So schützt F-Secure Internet Security 2003 Ihren Computer*. Definiert die Gefahren für Ihren Computer und erklärt, wie F-Secure Internet Security 2003 Ihren Computer gegen diese Bedrohungen schützt.

Fehlerbehebung - löst allgemeine Probleme.

Glossar - Terminologie.

Kundendienst und Wartung - enthält Kontaktinformationen, wenn Sie Unterstützung benötigen.

Symbolglossar

Die folgenden Symbole werden bei F-Secure Internet Security 2003 verwendet:

	Aktiviert	Diese Funktion ist aktiviert und funktioniert fehlerfrei.
	Frage	Eine Frage, durch die Sie u. U. zu einer Entscheidung aufgefordert werden.
	Info	Informativer Text zur Unterstützung bei der Verwendung von F-Secure Internet Security 2003.
	Ausgelastet	Warten Sie einen Moment.
	Warnung	Eine Funktion von F-Secure Internet Security 2003 ist deaktiviert, oder Ihre Virendefinitionen wurden seit längerem nicht aktualisiert.
	Fehler	Ein Fehler ist aufgetreten. Lesen Sie die Fehlermeldung sorgfältig durch.

Hinweis: Einige Symbolbedeutungen unterscheiden sich von denen auf der Seite „Meine Anmeldung“. Weitere Informationen finden Sie unter **Kapitel 7.** *Meine Anmeldung*. auf Seite 133.

1.F-Secure Internet Security 2003 installieren

1.1 Vor der Installation

Systemanforderungen

Ihr Computer muss den folgenden Anforderungen entsprechen, damit F-Secure Internet Security 2003 installiert und ausgeführt werden kann:

Prozessor:	Intel Pentium II oder höher
Betriebssystem:	Microsoft® Windows® 95/98/ME/NT 4.0 (SP6 erforderlich)/2000/XP
Arbeitsspeicher:	Windows 95/98/ME/NT 4.0: 64 MB RAM Windows 2000/XP: 128 MB RAM
Festplattenspeicher:	30 MB freie Speicherkapazität auf der Festplatte (60 MB bei der Installation)
Bildschirm:	Mindestens 256 Farben
Internetverbindung:	Eine Internetverbindung ist zur Validierung Ihrer Anmeldung und zum Empfangen von Aktualisierungen erforderlich.
Browser:	Internet Explorer 3.0 oder höher

Computer für die Installation vorbereiten

Das gleichzeitige Ausführen verschiedener Anti-Virus- und Firewall-Programme wird nicht empfohlen. Durch Konflikte zwischen Anti-Virus-Software können Ihre Dateien unter Umständen beschädigt werden.

Andere Anti-Virus- bzw. Firewall-Software entfernen

F-Secure Internet Security 2003 kann die Versionen F-Secure Anti-Virus 4 und 5 sowie F-Secure Distributed Firewall 5 automatisch aktualisieren.

Anti-Virus- und Firewall-Programme von anderen Herstellern müssen einzeln deinstalliert werden, bevor F-Secure Internet Security 2003 installiert werden kann. Anweisungen zum Deinstallieren der Software finden Sie in den entsprechenden Dokumentationen dieser Hersteller.

1.2 Installationsschritte

Hinweis: Wenn Sie Windows NT 4.0, Windows 2000 oder Windows XP verwenden und über mehr als ein Benutzerkonto verfügen, müssen Sie sich zur Installation von F-Secure Internet Security 2003 als Administrator anmelden.

Führen Sie zur Installation von F-Secure Internet Security 2003 die folgenden Schritte aus:

Teil 1: F-Secure Internet Security 2003 installieren

1. Führen Sie je nach Installationsmethode einen der folgenden Schritte aus:
   - Legen Sie die F-Secure Internet Security 2003-CD in das CD-ROM-Laufwerk Ihres Computers ein.

     Der Installationsvorgang wird automatisch gestartet. Wenn die CD nicht automatisch gestartet wird, suchen Sie auf der CD nach dem Setup-Verzeichnis, und öffnen Sie es. Suchen Sie die Datei INSTALL.EXE, und doppelklicken Sie darauf, um die Installation zu starten.
   - Laden Sie das Software-Paket auf Ihren Computer herunter. Schließen Sie alle anderen Programme, und führen Sie das Software-Paket zum Starten der Installation aus.
2. Schließen Sie alle anderen Programme, und legen Sie die F-Secure Internet Security 2003-CD in das CD-ROM-Laufwerk Ihres Computers ein.

   Der Installationsvorgang wird automatisch gestartet. Wenn die CD nicht automatisch gestartet wird, suchen Sie auf der CD nach dem Setup-Verzeichnis, und öffnen Sie es. Suchen Sie die Datei *INSTALL.EXE*, und doppelklicken Sie darauf, um die Installation zu starten.
3. Wählen Sie die Sprache, in der die Installation ausgeführt werden soll, und klicken Sie auf **Weiter**.
4. Lesen Sie die Anmeldungsvereinbarung durch, und aktivieren Sie das Kontrollkästchen *Ich akzeptiere die Vereinbarung*, wenn Sie den Bedingungen zustimmen. Klicken Sie auf **Weiter**, um fortzufahren.
5. Wählen Sie das Verzeichnis, in dem F-Secure Internet Security 2003 installiert werden soll. Klicken Sie auf **Weiter**, um fortzufahren.
6. Die Dateien werden auf Ihren Computer übertragen. Wenn die Übertragung abgeschlossen ist, fahren Sie mit dem zweiten Teil der Installation fort.

Hinweis: Sie werden unter Umständen aufgefordert, Ihren Computer neu zu starten. Wählen Sie *Jetzt neu starten* (wenn Sie *Später neu starten* wählen, wird die Installation erst fortgesetzt, wenn der Computer neu gestartet wurde), und klicken Sie auf **Fertig stellen**.

Teil 2: Komponenten auswählen und die Anmeldung validieren

1. Stellen Sie zur Validierung Ihrer Anmeldung sicher, dass Ihre Internetverbindung aktiv ist. Sie werden zu einem der folgenden Schritte aufgefordert:

- Geben Sie Ihre Anmeldungsnummer ein, um Ihre Anmeldung zu registrieren. Klicken Sie auf **Weiter**, um fortzufahren.
- Wählen Sie aus, dass das Produkt getestet werden soll (wenn Sie im Testmodus installieren). Klicken Sie auf **Weiter**, um fortzufahren. Wählen Sie im folgenden Fenster den gewünschten Installationstyp aus, und klicken Sie auf **Weiter**.

Tipp: Sie können den Installationsprozess verfolgen, wenn Sie in der Windows-Systemleiste rechts unten auf dem Bildschirm auf  doppelklicken. Das Symbol wird durch  ersetzt, sobald die Installation abgeschlossen ist.

Wenn Sie Komponenten vom Internet herunterladen, warten Sie, bis der Netzwerk-Installer alle Pakete heruntergeladen hat. Dies dauert gewöhnlich zwischen weniger als zwanzig Minuten mit einer ADSL-Verbindung und mehr als einer Stunde mit einem schnellen Modem.

2. Nachdem F-Secure Internet Security 2003 die erforderlichen Dateien installiert hat, werden Sie aufgefordert, den Computer neu zu starten. Wählen Sie *Jetzt neu starten* (wenn Sie *Später neu starten* wählen, wird die Installation erst abgeschlossen, wenn der Computer neu gestartet wurde). Klicken Sie auf **OK**, um die Installation abzuschließen.

   Unter *"Ist F-Secure Internet Security 2003 aktiv, und wird es einwandfrei ausgeführt?"* auf Seite 104 erfahren Sie, wie sich feststellen lässt, ob die Installation erfolgreich war.

Hinweis: Nach Abschluss der Installation werden Sie unter Umständen durch die Anwendungssteuerung dazu aufgefordert, festzulegen, über welche Anwendungen eine Verbindung zum Internet hergestellt werden soll und über welche nicht. Weitere Informationen hierzu finden Sie unter *"Vorgehensweise bei Anzeige des Anwendungssteuerungs-Popups"* auf Seite 103.

1.3 F-Secure Internet Security 2003 deinstallieren

Deinstallieren Sie F-Secure Internet Security 2003 mithilfe der Windows-Option *Software* in der Windows-Systemsteuerung. Hierdurch wird das Programm sicher und vollständig von Ihrem Computer entfernt. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie in der Windows-Taskleiste das Startmenü.
2. Wählen Sie *Einstellungen -> Systemsteuerung -> Software*.
3. Wählen Sie *F-Secure Internet Security 2003*, und klicken Sie auf **Entfernen**.
4. Starten Sie den Computer neu.

2. Erste Schritte

2.1 F-Secure Internet Security 2003 erstmalig verwenden

Wenn Sie F-Secure Internet Security 2003 erstmalig verwenden, lesen Sie sich die folgenden Abschnitte aufmerksam durch, um zu überprüfen, ob F-Secure Internet Security 2003 einwandfrei ausgeführt wird und Ihre Sicherheitsanforderungen erfüllt.

- Abschnitt 2.2 *Vorgehensweise bei Anzeige des Anwendungssteuerungs-Popups*.
- Abschnitt 2.3 *Ist F-Secure Internet Security 2003 aktiv, und wird es einwandfrei ausgeführt?*
- Abschnitt 2.4 *Optionen zum Zugriff auf F-Secure Internet Security 2003*.

2.2 Vorgehensweise bei Anzeige des Anwendungssteuerungs-Popups

Wenn F-Secure Internet Security 2003 installiert ist, wird je nach Internet Shield-Profil beim Herstellen einer Internetverbindung unter Umständen eine Anwendungssteuerungs-Meldung angezeigt.

Die Anwendungssteuerung ermöglicht sicheres Browsen und bietet einen hervorragenden Schutz vor bösartigen Programmen wie beispielsweise Trojanischen Pferden (Definitionen zu Trojanischen Pferden und anderen Stichwörtern finden Sie im *Glossar* auf Seite 143). Sie führt jedoch anfänglich zu einer Reihe von Aufforderungen zum Verhindern oder Zulassen von Verbindungen zu bestimmten Adressen. Die Zahl der Aufforderungen nimmt ab, und nachfolgend werden Ihnen nur noch selten Anwendungssteuerungs-Popups angezeigt, es sei denn, Sie installieren neue Software oder eine bösartige Anwendung versucht, eine Verbindung zwischen Ihrem Computer und dem Internet herzustellen.

Beispiel: Den Internet-Browser nach der Installation erstmalig starten

1. Starten Sie Ihren Internet-Browser (z. B. Internet Explorer, Netscape).

2. Das Anwendungssteuerungs-Popup wird angezeigt, in dem Sie angeben müssen, ob der Verbindungsversuch von Internet Explorer zugelassen oder verhindert werden soll.
   a. Wählen Sie *Diese Einstellung für die Zukunft speichern*, da Ihr Internet-Browser eine sichere Anwendung ist.
   b. Klicken Sie auf die Option zum Zulassen, da der von Ihnen selbst gestartete Browser sicher ist (weitere Informationen dazu, was als sicher bzw. nicht sicher gilt, finden Sie unter *„Verwendung der Anwendungssteuerung“* auf Seite 122).

Wenn Sie auf **Hilfe** klicken, werden weitere Informationen zur Anwendungssteuerung angezeigt.

Hinweis: Wenn Sie die Anwendungssteuerungs-Funktion deaktivieren möchten, rufen Sie die Internet Shield-Seite auf. Klicken Sie neben der Anwendungssteuerung auf **Ändern**. Der Statustext wird vom Anzeigen einer Eingabeaufforderung zu *Zulassen und protokollieren* geändert.

Weitere Informationen zur Anwendungssteuerung finden Sie unter *„Verwendung der Anwendungssteuerung“* auf Seite 122.

2.3 Ist F-Secure Internet Security 2003 aktiv, und wird es einwandfrei ausgeführt?

Nach der Installation bzw. bei der Verwendung von F-Secure Internet Security 2003 können Sie am Symbol in der rechten unteren Ecke der Windows-Systemleiste (wie nachfolgend dargestellt) sehen, ob F-Secure Internet Security 2003 aktiv ist und einwandfrei ausgeführt wird:

Hinweis: Unter Windows XP können Symbole ausgeblendet werden. Um ausgeblendete Symbole anzuzeigen, klicken Sie auf die Schaltfläche .

Je nach Status von F-Secure Internet Security 2003 wird das Symbol unter Umständen anders oder gar nicht angezeigt. In der folgenden Tabelle finden Sie eine Übersicht der Symbole und ihrer Bedeutungen:

Symbol	Bedeutung	Vorgehensweise
	F-Secure Internet Security 2003 wird einwandfrei ausgeführt. Ihr Computer ist geschützt.	Verwenden Sie Ihre E-Mail-Anwendung und Ihren Internet-Browser wie gewohnt.

Symbol	Bedeutung	Vorgehensweise
	Installation wird ausgeführt. Ihr Computer ist noch nicht geschützt.	Warten Sie, bis der Installationsvorgang abgeschlossen ist. Wenn die Installation abgeschlossen ist, wird das Symbol  angezeigt.
	Fehlerstatus. In F-Secure Internet Security 2003 ist ein Fehler aufgetreten.	Platzieren Sie Ihren Mauszeiger über dem Symbol  , um die Ursache für den Fehler anzuzeigen. Starten Sie den Computer gegebenenfalls neu.
	Warnung: Eine Schutzfunktion wurde deaktiviert, oder Ihre Virusdefinitionen sind nicht mehr aktuell. Ihr Computer ist nicht vollständig geschützt.	Platzieren Sie Ihren Mauszeiger über dem Symbol  , um die Informationen zum Status anzuzeigen. Aktivieren Sie die derzeit deaktivierte Funktion, oder rufen Sie F-Secure Internet Security 2003 auf, um nach Aktualisierungen zu suchen.
	Nicht geladen. F-Secure Internet Security 2003 ist deaktiviert, und Ihr Computer nicht geschützt.	Klicken Sie mit der rechten Maustaste auf das Symbol  , und wählen Sie die Option zum erneuten Laden aus, um F-Secure Internet Security 2003 zu aktivieren.
Kein Symbol	F-Secure Internet Security 2003 ist nicht installiert. Ihr Computer ist nicht geschützt.	Starten Sie Ihren Computer neu, und installieren Sie F-Secure Internet Security 2003.

2.4 Optionen zum Zugriff auf F-Secure Internet Security 2003

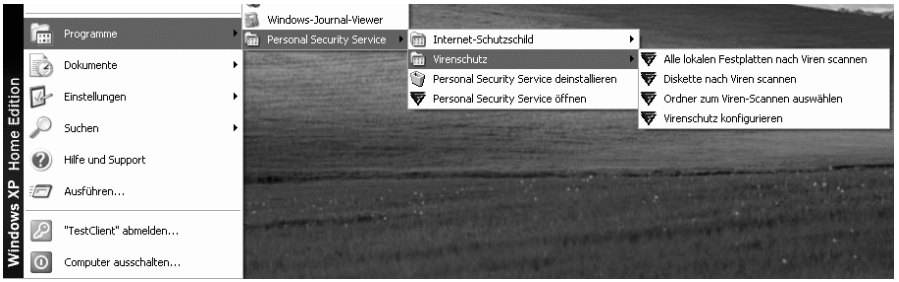
Es gibt mehrere Methoden zum Zugriff auf und zur Verwendung von F-Secure Internet Security 2003:

- Windows-Startmenü
- Symbol 
- F-Secure Internet Security 2003 Windows Explorer Popup-Menü

Windows-Startmenü

Führen Sie Folgendes aus, um F-Secure Internet Security 2003 zu öffnen, einfache Aufgaben auszuführen und Handbücher und Webseiten anzuzeigen:

1. Öffnen Sie das Windows-Startmenü.
2. Wählen Sie das Menü *Programme* und dann das Untermenü für F-Secure Internet Security 2003.
3. Klicken Sie auf die Option zum Öffnen von F-Secure Internet Security 2003, um F-Secure Internet Security 2003 aufzurufen, oder wählen Sie eine andere Option aus dem Untermenü aus.



Symbol

Über das Symbol in der Windows-Systemleiste (in der rechten unteren Ecke des Bildschirms) können Sie F-Secure Internet Security 2003 aufrufen sowie dessen Status anzeigen oder auf das Popup-Menü von F-Secure Internet Security 2003 zugreifen.

Doppelklicken Sie zum Öffnen von F-Secure Internet Security 2003 mit der linken Maustaste auf das Symbol .

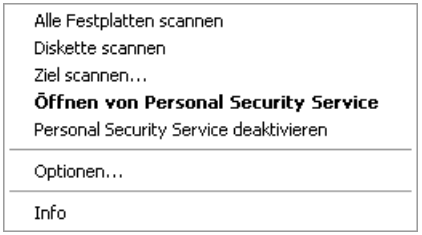
F-Secure Internet Security 2003 Statusinformationen

Platzieren Sie Ihre Maus über dem Symbol, um die Statusinformationen für F-Secure Internet Security 2003 anzuzeigen. Anhand dieser Informationen können Sie sofort erkennen, ob bei F-Secure Internet Security 2003 ein Problem vorliegt (wie im nachfolgenden Beispiel, in dem der Virenschutz deaktiviert wurde).

F-Secure Internet Security 2003 Popup-Menü

Klicken Sie mit der rechten Maustaste auf das Symbol, um das Popup-Menü von F-Secure Internet Security 2003 aufzurufen, das eine Liste der am häufigsten verwendeten Aufgaben enthält. Von

diesem Menü aus können Sie F-Secure Internet Security 2003 öffnen oder direkt nach Viren scannen.



Die folgende Tabelle erläutert genau, was die einzelnen Menüelemente bedeuten:

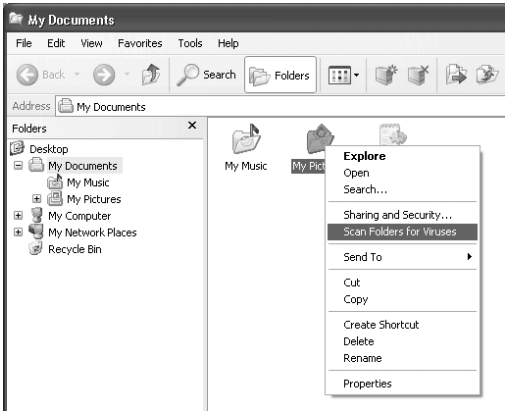
Option	Erklärung
Option zum Öffnen von F-Secure Internet Security 2003	Öffnet F-Secure Internet Security 2003.
F-Secure-Produkte entladen	Löscht Produkte aus dem Speicher. Dies ist unter Umständen erforderlich, wenn Software installiert wird oder leistungskritische Aufgaben ausgeführt werden. Ihr Computer sollte nicht über längere Zeiträume in diesem Status verbleiben, da er hierbei nicht geschützt ist.
Alle Festplatten scannen	Der Virenschutz scannt alle verfügbaren Festplatten auf Ihrem Computer.
Diskette scannen	Der Virenschutz scannt alle Disketten im Laufwerk A:.
Ziel scannen…	Der Virenschutz scannt das von Ihnen angegebene Ziel. Ein Verzeichnisbaum wird angezeigt. Wählen Sie Ihr Zielverzeichnis aus, und klicken Sie auf **OK**, um den Scanvorgang zu starten.
Optionen…	Öffnet erweiterte Optionen.
Info...	Zeigt Informationen zu F-Secure Internet Security 2003 an.

F-Secure Internet Security 2003 Windows Explorer Popup-Menü

Mit Windows Explorer können Sie Laufwerke, Ordner und Dateien auf Viren scannen. Gehen Sie dazu folgendermaßen vor:

1. Platzieren Sie Ihren Mauszeiger auf dem zu scannenden Laufwerk oder Ordner bzw. der zu scannenden Datei, und klicken Sie mit der rechten Maustaste.

2. Wählen Sie aus dem Popup-Menü **Ordner nach Viren scannen** aus. Das Fenster für manuelles Scannen wird angezeigt und der Scanvorgang gestartet.



Für den Fall, dass ein Virus gefunden wird, lesen Sie unter *„Viren vom Computer entfernen“* auf Seite 113 weiter.

Hinweis: Wenn Sie einen Scan ausführen, verwendet F-Secure Internet Security 2003 zum Scannen die Einstellungen aus dem aktuellen Virenschutzprofil. Siehe *„Virenschutzprofile ändern“* auf Seite 112.

3. Homepage

Die *Homepage* bietet eine detaillierte Übersicht zu Ihren Sicherheitseinstellungen und dem Status von F-Secure Internet Security 2003.

Auf der Homepage stehen Ihnen folgende Optionen zur Verfügung:

- Auswählen des Virenschutzprofils und Überwachen des Virenschutzstatus. Weitere Information und Anweisungen finden Sie im **Kapitel 4.** *Virenschutz*.
- Auswählen des Internet Shield-Profils. Weitere Information und Anweisungen finden Sie im **Kapitel 5.** *Internet Shield*.
- Aktivieren und Deaktivieren der automatischen Aktualisierungen sowie Anzeigen von Informationen zu den auf Ihren Computer heruntergeladenen Aktualisierungen. Weitere Informationen und Anweisungen finden Sie im **Kapitel 6.** *Automatische Aktualisierungen*.

4. Virenschutz

Auf der Virenschutzseite können Sie Folgendes ausführen:

- Ihr Virenschutzprofil auswählen (weitere Informationen finden Sie unter *„Virenschutzprofile“* auf Seite 111).
- Überprüfen, wann Sie Aktualisierungen zu Virusdefinitionen erhalten haben und wann Ihre Virusdefinitionsdateien im F-Secure VirusLab erstellt wurden.
- Überprüfen, wie viele Dateien von F-Secure Internet Security 2003 gescannt und wie viele Viren entfernt wurden.
- Manuell nach Viren scannen (weitere Informationen hierzu finden Sie unter *„Nach Viren scannen“* auf Seite 112).

4.1 Virenschutzprofile

Mithilfe von Virenschutzprofilen können Sie je nach aktuellen Anforderungen direkt und unverzüglich den Umfang ändern, in dem Ihre Daten und Ihr System geschützt werden. Profile werden automatisch aktualisiert, damit Sie jederzeit gegen neue Arten bösartiger Computerprogramme und Internetangriffe geschützt sind.

Wenn Sie in einem Profil eine beliebige Einstellung ändern (über die **Erweiterten Einstellungen** von Virus Protection), wird dessen Name zu „Benutzerdefiniert“ geändert. Informationen zum Wiederherstellen Ihres Virenschutzprofils finden Sie unter „*Virenschutzprofile ändern*“ weiter unten.

Virenschutzprofile ändern

Sie können die Profile jederzeit je nach aktuellen Sicherheitsanforderungen ändern. Durch das Ändern des ausgewählten Profils wird die Sicherheitsstufe für automatisierte Vorgänge und Berichtsfunktionen geändert.

So ändern Sie Ihr Profil im Virenschutzabschnitt:

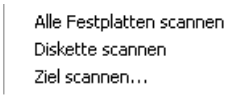
1. Klicken Sie auf **Ändern**.
2. Wählen Sie ein Profil aus der Dropdown-Liste aus. Lesen Sie sich die angezeigte Beschreibung eines Profils aufmerksam durch, bevor Sie es aktivieren.
3. Klicken Sie auf **OK** , um das ausgewählte Profil zu verwenden.

4.2 Nach Viren scannen

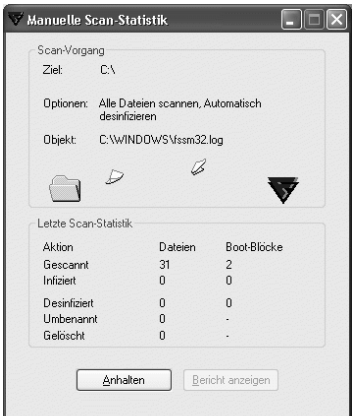
Bei aktiviertem Virenschutz ist Ihr Computer geschützt. Beim Öffnen oder Schließen von Dateien werden diese automatisch nach Viren gescannt.

Wenn Sie den Verdacht haben, dass eine bestimmte Datei einen Virus enthält, können Sie nur diese Datei oder auch Ihren gesamten Computer nach Viren scannen. Gehen Sie zum Scannen folgendermaßen vor:

1. Klicken Sie auf die Schaltfläche zum Scannen nach Viren.
2. Wählen Sie aus dem Menü aus, dass alle lokalen Festplatten, eine Diskette oder ein bestimmter Ordner gescannt werden sollen.



3. Das Fenster *Manuelle Scan-Statistik* wird angezeigt, in dem die Statistikwerte für den Scan aufgeführt sind. Klicken Sie auf **Anhalten**, um den Scan zu unterbrechen.



4. Nach Abschluss des Scan-Vorgangs wird ein Bericht erstellt. Klicken Sie auf **Bericht anzeigen**, um den Bericht im Web-Browser anzeigen zu lassen. Für den Fall, dass ein Virus gefunden wird, lesen Sie unter *„Viren vom Computer entfernen“* auf Seite 113 weiter.

Hinweis: Wenn Sie einen Scan ausführen, verwendet F-Secure Internet Security 2003 die Einstellungen aus dem aktuellen Virenschutzprofil. Weitere Informationen zum Auswählen eines anderen Profils finden Sie unter *„Virenschutzprofile“* auf Seite 111.

4.3 Viren vom Computer entfernen

So entfernt der Desinfektions-Assistent von F-Secure Anti-Virus einen gefundenen Virus

Der Desinfektions-Assistent von F-Secure Anti-Virus wird angezeigt, wenn:

- beim Virus-Scan ein Virus gefunden wurde.
- ein Virus gefunden wurde und Ihr Virenschutzprofil darauf eingestellt ist, alle Ergebnisse anzuzeigen und Sie vor der Desinfektion zu benachrichtigen.
- bei einem automatischen Scan ein Virus gefunden wurde (automatischer Schutz ist aktiviert) und F-Secure Internet Security 2003 den Virus nicht selbst entfernen konnte.

Befolgen Sie zum Entfernen des Virus die folgenden Schritte.

Schritt 1: Virus festgestellt

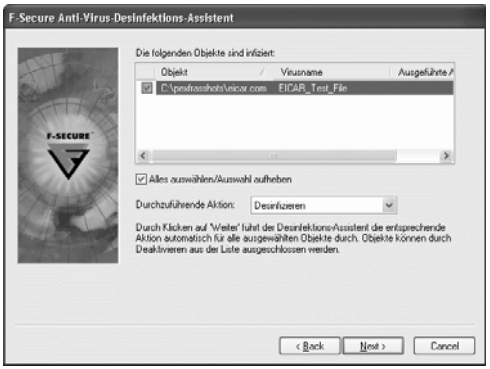
Der Name des gefundenen Virus wird wie unten angegeben angezeigt. Klicken Sie auf **Weiter**, um mit der Virendesinfektion fortzufahren.

Hinweis: Weitere Informationen zum Virus erhalten Sie, indem Sie auf den Namen des Virus und anschließend auf die Schaltfläche **Vireninfo** klicken. Falls es sich um einen neuen Virus handelt, ist er unter Umständen in der Datenbank noch nicht aufgeführt. Suchen Sie im F-Secure Computerviren-Infocenter unter http://www.f-secure.com/v-descs/ nach den aktuellsten Informationen.

Schritt 2: Durchgeführte Aktion

Eine Liste mit infizierten Dateien wird angezeigt.

Wählen Sie im Feld **Durchzuführende Aktion** die Aktion aus, die hinsichtlich der infizierten Dateien



durchgeführt werden soll. In der nachfolgenden Tabelle finden Sie eine Übersicht über die einzelnen Aktionen.

Aktion	Erklärung
Desinfizieren	Der Desinfektions-Assistent desinfiziert die infizierte Datei. **Hinweis:** Wenn der Desinfektions-Assistent die Datei nicht desinfizieren kann, versucht er, sie automatisch umzubenennen.

Aktion	Erklärung
Löschen	Der Desinfektions-Assistent löscht die Datei, die den Virus enthält. Alle Daten aus dieser Datei gehen dabei verloren. **Warnung:** Wenn Sie auf **Löschen** klicken, wird auch das infizierte Objekt gelöscht.
Umbenennen	Der Desinfektions-Assistent benennt die Datei um, so dass diese nicht automatisch ausgeführt werden kann. Dadurch wird verhindert, dass der Virus aktiviert wird.

Klicken Sie, nachdem Sie die auszuführende Aktion ausgewählt haben, auf **Weiter**. Dadurch führt der Desinfektions-Assistent die Aktion automatisch für alle ausgewählten Objekte durch.

Schritt 3: Aktionsergebnisse

Das Ergebnis der Aktion wird angezeigt. Wenn die von Ihnen ausgewählte Aktion fehlgeschlagen ist, können Sie Schritt 2 wiederholen und eine andere Aktion auswählen.

Wenn Desinfektions- oder Löschaktionen fehlschlagen, können Sie die Datei auch umbenennen. Dies ist normalerweise bei infizierten ausführbaren Dateien (.EXE-Dateien) ratsam, da durch die Umbenennung die Erweiterung so geändert wird, dass diese Dateien nicht automatisch ausgeführt werden können.

Beachten Sie beim Fehlschlagen von Desinfektionsaktionen, dass der Desinfektions-Assistent die Datei unter Umständen bereits automatisch umbenannt hat (siehe Aktionstabelle oben). Ein Hinweis darauf wird im Feld *Eigenschaften* angezeigt.

Hinweis: Wenn ein neuer Virus gefunden wurde, die Virusdefinitionen veraltet sind oder ein falscher Alarm ausgegeben wird, kann die Desinfektion oder das Löschen fehlschlagen. Anleitungen dazu, was in einem solchen Fall zu tun ist, finden Sie unter *„Viren nach Fehlschlagen des Desinfektions-Assistenten entfernen“* auf Seite 116.

Wenn die Aktion erfolgreich war, klicken Sie auf **Weiter**, um fortzufahren.

Schritt 4: Prüfen und Abschließen

Nachdem der Desinfektionsvorgang abgeschlossen ist, wird ein Desinfektionsbericht erstellt. Wenn Sie nicht möchten, dass ein Bericht erstellt wird, deaktivieren Sie das Kontrollkästchen **Bericht erstellen**. Beachten Sie, dass der Desinfektionsbericht nicht für Viren erstellt wird, die während eines automatischen Scans gefunden wurden.

Klicken Sie auf **Fertig stellen**, um den Desinfektions-Assistenten zu schließen.

Der Desinfektionsbericht wird in Ihrem Standard-Web-Browser angezeigt und enthält Verknüpfungen zu entsprechenden Virenbeschreibungen in der Virendatenbank des Web-Clubs.

Hinweis: Wenn der Virus in einer Datei gefunden wurde, die beim Löschversuch des Desinfektions-Assistenten durch einen anderen Vorgang gesperrt war, wird ein Fenster angezeigt, das Sie zum Neustart des Computers auffordert. Wenn dieses Fenster angezeigt wird, speichern Sie alle Dokumente, und führen Sie dann die im Fenster angezeigten Anweisungen aus.

Viren nach Fehlschlagen des Desinfektions-Assistenten entfernen

Wenn der Desinfektions-Assistent die Datei nicht desinfizieren bzw. löschen konnte, hat dies unter Umständen eine der folgenden Ursachen:

- Die Virusdefinitionsdatenbank ist veraltet. Überprüfen Sie, ob Sie über die aktuellsten Definitionsdateien verfügen, und versuchen Sie es erneut (siehe **Kapitel 6.** *Automatische Aktualisierungen*.).
- Falscher Alarm. Es wurden umfassende Vorkehrungen getroffen, um sicherzustellen, dass F-Secure Internet Security 2003 keine harmlosen Dateien als infiziert anzeigt; aufgrund der Komplexität von Dateien kann dies jedoch unter Umständen vorkommen.
- Es ist eine manuelle Desinfektion erforderlich. In einigen Fällen müssen Sie ein Programm ausführen, das die Datei desinfiziert und den Virus entfernt. Dieser Fall tritt häufig bei neueren Viren ein, die sich mithilfe raffinierter Techniken verstecken und an Ihre Dateien anhängen.
- Sie haben einen neuen Virus entdeckt. Ihr Computer ist unter Umständen durch einen neuen Virus infiziert worden. Kein Grund zur Panik. Ihre Dateien sind geschützt, da F-Secure Internet Security 2003 den Virus entdeckt und gestoppt hat, bevor dieser Schaden anrichten konnte.

Wenn Sie sich sicher sind, dass die Datei nicht infiziert ist, können Sie die Warnungen ignorieren. Sie können den automatischen Schutz und manuelles Scannen konfigurieren, um diese Datei bei zukünftigen Scans zu übergehen. Anweisungen dazu finden Sie unter *„Schutzeinstellungen zum Ignorieren/Scannen ausgewählter Dateien aktivieren“* auf Seite 118.

Manuelles Entfernen von Viren

1. Versuchen Sie, die Datei selbst zu desinfizieren. Weitere Hilfe zum Entfernen des Virus finden Sie auch hier:
   - Suchen Sie im F-Secure Computerviren-Infocenter unter http://www.f-secure.com/v-descs/ nach Informationen zu den Viren. Die Vireninformationen erleichtern Ihnen das Entfernen des Virus und enthalten unter Umständen Verknüpfungen zu den für das Entfernen erforderlichen Programmen.
   - Erfahrene Benutzer: Geeignete Desinfektionsprogramme finden Sie direkt unter ftp://ftp.europe.f-secure.com/anti-virus/tools/.

   Die Programme enthalten alle erforderlichen Anweisungen, die Sie zum Entfernen des Virus aus Ihrem System ausführen müssen.
2. Wenn der Desinfektions-Assistent fehlgeschlagen ist, Ihre Virusdefinitionsdatenbank auf dem aktuellsten Stand ist und das Ausführen von Desinfektionsprogrammen von der F-Secure Website erfolglos war, befolgen Sie die Anweisungen unter *„Vorgehensweise bei Feststellen eines neuen Virus“* auf Seite 117.

4.4 Vorgehensweise bei Feststellen eines neuen Virus

Wenn F-Secure Internet Security 2003 eine Warnung anzeigt, dass eine Datei mit einem Virus infiziert ist, aber den Virus nicht benennen und nicht desinfizieren oder entfernen kann, handelt es sich unter Umständen um einen neuen Virus. Sie sollten diese Datei erst wieder verwenden, wenn Sie sicher sind, dass der Virus entfernt wurde, bzw. wenn klar ist, dass ein falscher Alarm vorlag.

Führen Sie zum Entfernen des Virus die folgenden Schritte aus:

1. Überprüfen Sie, ob Ihre Virusdefinitionsdatenbank auf dem aktuellsten Stand ist. Eine aktuellere Definitionsdatei stellt F-Secure Internet Security 2003 unter Umständen die Informationen zur Verfügung, die zum Entfernen des Virus von Ihrem Computer benötigt werden.
2. Wenn Sie bereits über die aktuellsten Virusdefinitionen verfügen (siehe **Kapitel 6.** *Automatische Aktualisierungen*.), suchen Sie auf der F-Secure Website nach Programmen, mit denen Sie den Virus manuell entfernen können (http://www.f-secure.com/v-descs/ bzw. ftp://ftp.europe.f-secure.com/anti-virus/tools/).
3. Wenn die oben aufgeführten Schritte fehlschlagen, senden Sie die Datei an das F-Secure VirusLab. Anweisungen hierzu finden Sie unter:

   http://www.f-secure.com/support/technical/general/samples.shtml.

4.5 Schutzeinstellungen zum Ignorieren/Scannen ausgewählter Dateien aktivieren

In bestimmten Fällen ist es ratsam, den Virenschutz einzustellen, um bestimmte Dateitypen bzw. bestimmte Dateien zu ignorieren. Beispielsweise, wenn Folgendes der Fall ist:

- Sie sind sicher, dass eine Datei nicht infiziert ist und ein falscher Alarm vorliegt.
- Ihr Computer ist weitgehend ausgelastet, und das Einstellen des Virenschutzes auf das Scannen aller Dateien würde die Arbeitsprozesse Ihres Computers erheblich verlangsamen und so ein Arbeiten unmöglich machen.
- Die Datei hat einen Dateityp, der nie durch Viren infiziert wird.

Bei einigen Profilen sind die Scan-Einstellungen bereits so eingestellt, dass nur bestimmte Dateitypen gescannt werden. Dadurch wird gewährleistet, dass hauptsächlich Dateien gescannt werden, die üblicherweise von Viren infiziert werden, so dass der Prozessor und Speicher nicht unnötig belegt werden.

Warnung: Wenn der Virenschutz darauf eingestellt wird, bestimmte Dateien zu ignorieren, bedeutet dies, dass diese Dateien für zukünftige Virusangriffe anfällig sind und der Virus-Scan Viren unter Umständen nicht finden oder desinfizieren kann. Dies wird nur empfohlen, wenn es zwingend notwendig ist.

Echtzeitschutz oder manuelles Scannen zum Scannen ausgewählter Dateien einstellen

So stellen Sie den Echtzeitschutz oder das manuelle Scannen zum Scannen ausgewählter Dateien ein:

1. Öffnen Sie das Hauptfenster von F-Secure Internet Security 2003.
2. Wählen Sie die Virenschutzseite, und klicken Sie auf **Erweiterte Einstellungen**. Prüfen Sie, dass auf den Registerkarten für den Echtzeitschutz und das manuelle Scannen **Dateien mit diesen Erweiterungen** aktiviert ist.

Echtzeitschutz oder manuelles Scannen zum Ignorieren ausgewählter Dateien einstellen

So stellen Sie den Echtzeitschutz oder das manuelle Scannen zum Ignorieren ausgewählter Dateien ein:

1. Öffnen Sie das Hauptfenster von F-Secure Internet Security 2003.
2. Wählen Sie die Virenschutzseite, und klicken Sie auf **Erweiterte Einstellungen**. Prüfen Sie, dass auf den Registerkarten für den Echtzeitschutz und das manuelle Scannen Folgendes gilt:
   - **Dateien mit diesen Erweiterungen ausschließen** ist aktiviert. Geben Sie im Textfeld die Dateierweiterungen ein.
   - **Objekte ausschließen (Dateien, Ordner, …)** ist aktiviert. Klicken Sie auf **Auswählen**, um die Dateien auszuwählen, die Sie ausschließen möchten, und fügen Sie diese zur Liste der auszuschließenden Dateien hinzu.

5. Internet Shield

Auf der Seite zum Internet Shield können Sie Folgendes ausführen:

- Internet Shield-Profil auswählen (weitere Informationen finden Sie unter *„Internet Shield-Profile“* auf Seite 122).
- Status der Anwendungssteuerung ändern. Klicken Sie dazu neben dem aktuellen Status der Anwendungssteuerung auf die Schaltfläche **Ändern**.
- Überprüfen, wie viele Anwendungen zur Internetverbindung zugelassen oder abgelehnt werden. Informationen zum Ändern der Verbindungsrechte von Anwendungen finden Sie unter *„Ändern der Verbindungsrechte von Anwendungen“* auf Seite 122.
- Ihre Alarmkonfiguration ändern. Klicken Sie dazu neben dem aktuellen Status auf die Schaltfläche **Ändern**.
- Anzahl der Alarme anzeigen, die Sie seit einem bestimmten Zeitpunkt erhalten haben. Klicken Sie auf **Ansicht**, um die Liste mit den Alarmmeldungen anzuzeigen.
- Anzahl der abgebrochenen Paketübertragungen überprüfen. Die Übertragung bekannter gefährlicher Pakete wird stets von Internet Shield abgebrochen. Sie können allerdings das Abbrechen von Paketübertragungen beeinflussen, indem Sie Ihre Richtlinien zum Internet Shield benutzerdefiniert anpassen (Anweisungen dazu finden Sie unter *„Anpassen von Internet Shield-Regeln“* auf Seite 124).

- Zeitpunkt des letzten Internet Shield-Alarms überprüfen. Klicken Sie auf **Details**, um Details zum letzten Alarm sowie die ersten fünf blockierten Protokolle und Hosts (IP-Adressen) anzuzeigen.

5.1 Internet Shield-Profile

Mit den Profilen für Internet Shield können Sie umgehend Ihre Schutzebene entsprechend Ihren Anforderungen ändern. Durch automatische Aktualisierungen wird darüber hinaus sichergestellt, dass Sie gegen die neuesten Arten von bösartigen Computer-Programmen und Internet-Angriffen geschützt werden.

Ändern Ihres Internet Shield-Profils

Sie können die Profile jederzeit je nach aktuellen Sicherheitsanforderungen ändern. Durch das Ändern des ausgewählten Profils wird die Sicherheitsstufe für automatisierte Vorgänge und Berichtsfunktionen geändert.

So ändern Sie Ihr Profil im Abschnitt zum Internet Shield:

1. Klicken Sie auf **Ändern**.
2. Wählen Sie ein Profil aus der Dropdown-Liste aus. Lesen Sie sich die Beschreibung eines Profils aufmerksam durch, bevor Sie es aktivieren.
3. Klicken Sie auf **OK**, um das ausgewählte Profil zu verwenden.

Weitere Informationen zur individuellen Anpassung eines Profils finden Sie unter *„Anpassen von Internet Shield-Regeln“* auf Seite 124.

5.2 Verwendung der Anwendungssteuerung

Die Anwendungssteuerung ist eine Funktion von F-Secure Internet Security 2003, mit der alle Anwendungen, die von Ihrem Computer aus mit dem Internet verbunden sind, überprüft werden. Bei der Anwendungssteuerung werden Sie gefragt, ob Sie den Verbindungsversuch der Anwendung zulassen oder ablehnen möchten. Dieser Vorgang wird im Abschnitt *„Vorgehensweise bei Anzeige des Anwendungssteuerungs-Popups“* auf Seite 103 beschrieben. Sichere und bekannte Anwendungen sollten zur Internet-Verbindung zugelassen, nicht vertrauenswürdige Anwendungen dagegen abgelehnt werden.

In der Aktionsprotokolldatei werden alle Verbindungen sowie deren Eigenschaften aufgeführt, so dass Sie sehen, welche Verbindungen Ihr Computer hergestellt hat. Um auf das Protokoll zuzugreifen, klicken Sie auf **Erweiterte Einstellungen** und anschließend auf die Registerkarte *Protokollfunktion*.

Ändern der Verbindungsrechte von Anwendungen

So ändern Sie die Verbindungsrechte bzw. Eigenschaften einer Anwendung:

1. Öffnen Sie die Internet Shield-Seite, und klicken Sie neben der Schaltfläche für *Anwendungen zugelassen/abgelehnt* auf **Ändern**.
2. Die Seite mit den Einstellungen zum *Internet Shield* wird geöffnet.

3. Wählen Sie die Anwendung aus, deren Eigenschaften Sie ändern möchten (die aktuellen Rechte sind in der Spalte mit den Rechten aufgeführt). Klicken Sie auf **Eigenschaften**.
4. Wählen Sie die Option **Ablehnen**, **Auffordern** bzw. **Zulassen** aus. Klicken Sie auf **OK**, um zur Anwendungsseite zurückzukehren.
5. Die neuen Rechte der Anwendung werden neben dem Anwendungsnamen in der Spalte mit den Rechten angezeigt. Klicken Sie auf **Schließen**, um den Vorgang zu beenden.

Was gilt als sicher?

- Eine bekannte Anwendung, die Sie selbst aktiv gestartet haben.
- Windows-Dienste, die eine Verbindung mit dem Internet herstellen.

Sichere Microsoft Windows-Dienste

Bei bestimmten Microsoft Windows-Diensten ist zum Betrieb ein Netzwerkzugriff erforderlich. Die meisten Dienste werden automatisch zugelassen, die Anwendungssteuerung kann jedoch u. U. eine Eingabeaufforderung für die unten aufgeführten Dienste anzeigen; dies ist vor allem der Fall beim Betrieb auf Windows NT 4.0-, Windows 2000- und Windows XP-Plattformen. Lassen Sie bei diesen Plattformen den Zugriff auf das Netzwerk zu, da andernfalls einige der Windows-Funktionen nicht ausgeführt werden können.

Anwendungsliste:

Hinweis: %Winnt% verweist auf das Installationsverzeichnis in Windows, normalerweise C:\Winnt\.

EXE-Datei	Pfad	Beschreibung	Netzwerk-Datenverkehr
SVCHOST.EXE	%Winnt%\System32\	Generisches Host-Verfahren für Win32-Dienste	udp/67 ausgehend, udp/68 eingehend, udp/137 ausgehend
SPOOLSV.EXE	%Winnt%\System32\	Spooler-Subsystem-Anwendung	udp/137 ausgehend, udp/138 ausgehend
LSASS.EXE	%\Windows%\System32\	LSA-EXE-Datei und Server-DLL	udp/137 ausgehend
SERVICES.EXE	%Winnt%\System32\	Dienste- und Controller-Anwendung	udp/67 ausgehend, udp/68 eingehend, udp/137 ausgehend
WINLOGON.EXE			udp/137 ausgehend

Was gilt als unsicher?

Anwendungen, die Sie von einer nicht vertrauenswürdigen Quelle empfangen haben, sollten immer mit Vorsicht behandelt werden. Anwendungen, die Sie von einer vertrauenswürdigen Quelle ohne vorherige Vereinbarung erhalten haben, sollten auch als verdächtig behandelt werden.

- Anwendungen, die Sie nicht selbst installieren haben oder die Ihnen unbekannt sind.
- Anwendungen, die als sicher gelten, aber die versuchen, eine Verbindung herzustellen, ohne dass Sie sie starten.
- Verbindungen, die keinen richtigen Zielnamen (Text-Webadresse) enthalten.

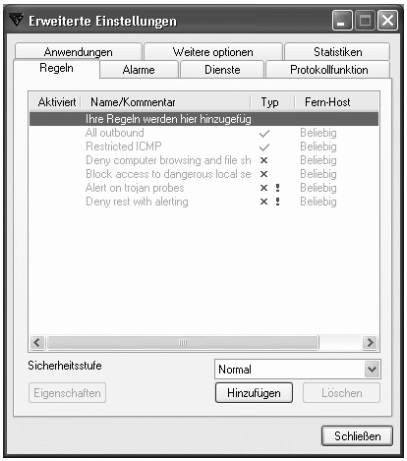
5.3 Anpassen von Internet Shield-Regeln

In einigen Situationen kann es erforderlich werden, dass Sie Regeln, die die Vorgehensweise bei bestimmten Verbindungen definieren, hinzufügen, ändern bzw. löschen möchten. Dieser Fall kann bei folgenden Vorgängen eintreten:

- Verbindungsherstellung zu einem neuen Spiele-Server auf einem bestimmten Computer.
- Zulassen allgemeiner Verbindungen, aber Blockieren einer Verbindung zu einer bestimmten Website bzw. einem Computer, der bzw. dem Sie nicht vertrauen.

So passen Sie Ihre Einstellungen von Internet Shield an:

1. Klicken Sie auf der Internet Shield-Seite auf die Option **Erweiterte Einstellungen**. Das Fenster **Erweiterte Einstellungen** wird angezeigt.
2. Wählen Sie im Pulldown-Menü **Sicherheitsstufe** das anzupassende Profil aus.
3. Klicken Sie auf die Registerkarte **Regeln** (wenn diese noch nicht ausgewählt wurde).



- Um eine bereits bestehende Regel zu ändern, wählen Sie diese aus der Liste aus, und klicken Sie auf **Eigenschaften**.
- Um eine neue Regel hinzuzufügen, klicken Sie auf **Hinzufügen**.
- Um eine Regel zu löschen, wählen Sie diese aus der Liste aus, und klicken Sie auf **Löschen**.

Hinweis: Vordefinierte Regeln können nicht geändert bzw. gelöscht werden. Sie können nur neue Regeln hinzufügen bzw. von Ihnen selbst hinzugefügte Regeln ändern und löschen.

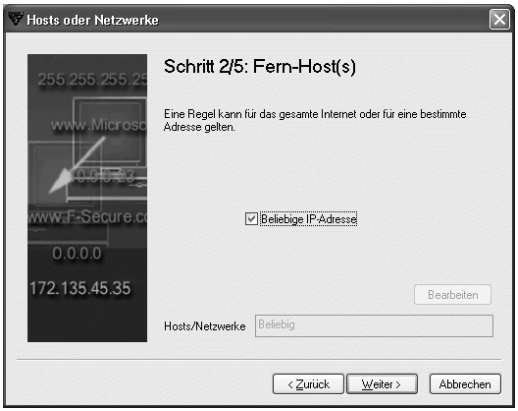
Erstellen von neuen Internet Shield-Regeln

Schritt 1: Regeltyp

Geben Sie der Regel einen beschreibenden Namen, und lassen Sie entweder die Verbindung zu oder lehnen diese ab.

Schritt 2: Geben Sie die Ziele an

Wählen Sie aus, ob Sie diese Regel auf alle Verbindungen oder nur auf bestimmte Verbindungen anwenden möchten.



Sie können folgende Möglichkeiten auswählen:

- Aktivieren Sie **Beliebige IP-Adresse**, um die Regel für alle Internet-Verbindungen anzuwenden, und klicken Sie auf **Weiter**, um mit Schritt 3 fortzufahren; oder
- deaktivieren Sie **Beliebige IP-Adresse**, und klicken Sie auf **Bearbeiten**, um ein neues Fenster zu öffnen, in dem Sie die Zieldetails eingeben können.
- Die Ziele können in beliebiger Reihenfolge und unabhängig vom Typ aufgeführt werden; das Ziel kann entweder ein DNS-Name, eine IP-Adresse, ein Teilnetz (im Bit-Netzmaskenformat) oder ein IP-Adressenbereich sein. Beispielsweise:

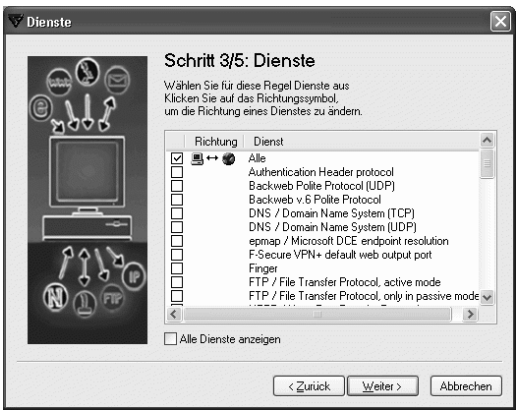
DNS-Name:	www.some.domain.org
IP-Adresse:	192.168.5.16
Teilnetz:	192.168.88.0/29
IP-Bereich:	192.168.1.1-192.168.1.63

Klicken Sie auf die Schaltfläche **Hinzufügen**, um das neue Ziel zur Liste der Ziele hinzuzufügen, auf die diese Regel angewendet wird. Um ein Ziel aus der Liste zu entfernen, wählen Sie es aus, und klicken Sie dann auf **Entfernen**. Um die Eigenschaften eines Ziels zu bearbeiten, wählen Sie aus der Liste die Zieladresse aus. Klicken Sie auf **OK**, um zur Seite mit den entfernten Hosts zu wechseln, und klicken Sie dann auf **Weiter**, um fortzufahren.

Schritt 3: Wählen Sie den Dienst und die Richtung für die Regel aus

Wählen Sie aus der Liste der verfügbaren Dienste den Dienst aus, für den diese Regel angewendet werden soll. Wenn die Regel auf alle Dienste angewendet werden soll, wählen Sie oben aus der Liste die Option *Alle* aus.

Sie können beliebig viele Einzeldienste auswählen.

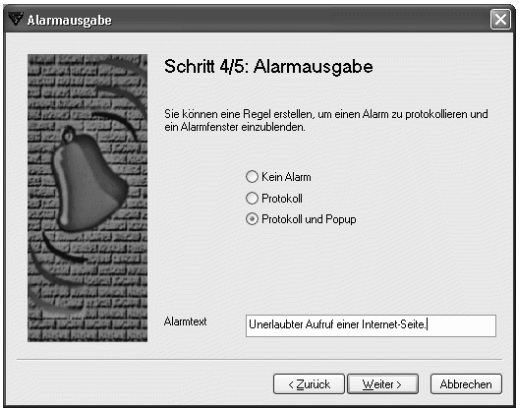


Wählen Sie für die ausgewählten Dienste die Richtung aus, in der die Regel angewendet wird, indem Sie auf das rote Fragezeichen klicken. Durch wiederholtes Klicken wechseln Sie zwischen den verfügbaren Optionen. In der unten stehenden Tabelle finden Sie einige Beispiele dazu.

Option	Begriff	Erklärung
	Undefiniert	Die Richtung wurde noch nicht definiert. Klicken Sie auf die Grafik, um eine Richtung zu definieren.
	Eingehend	Der Dienst wird zugelassen/abgelehnt, wenn Ihr Computer diesen vom Internet erhält.
	Ausgehend	Der Dienst wird zugelassen/abgelehnt, wenn Ihr Computer diesen ins Internet schickt.
	Beide	Der Dienst wird von Ihrem Computer aus in beide Richtungen zugelassen/abgelehnt.

Schritt 4: Wählen Sie die Protokoll- und Berichtsfunktion aus

Sie können auswählen, ob Sie informiert werden möchten, wenn die Regel auf eine versuchte Verbindung angewendet wird.



- *Kein Alarm* bedeutet, dass Ihnen nicht mitgeteilt wird, wenn die Regel auf eine Verbindung angewendet wird.
- *Protokoll* bedeutet, dass in einer Datei Daten zur Verbindung protokolliert werden.
- *Protokoll und Popup* bedeutet, dass Daten protokolliert werden und Ihnen in einem Popup-Fenster mitgeteilt wird, wenn beispielsweise die Verbindung zugelassen/abgelehnt wird.

Schritt 5: Überprüfen und akzeptieren Sie die Regel

Sie können jetzt Ihre Regel überprüfen. Klicken Sie auf **Zurück**, um an der Regel ggf. Änderungen vorzunehmen.

Wenn die Regel Ihrer Zufriedenheit entspricht, klicken Sie auf **Fertig stellen**. Ihre neue Regel wird im aktiven Regelsatz in der Registerkarte **Regeln** der Internet Shield-Einstellungen oben zur Liste hinzugefügt.

5.4 Erweiterte Einstellungen

Hinweis: Dieser Abschnitt richtet sich nur an erfahrene Computer-Benutzer. Internet Shield kann durch Änderung von Einstellungen deaktiviert werden.

Um auf die erweiterten Internet Shield-Einstellungen zuzugreifen, klicken Sie auf der Internet Shield-Seite auf die Option **Erweiterte Einstellungen**. Klicken Sie im daraufhin angezeigten Fenster auf die Registerkarte **Erweitert**.

Berücksichtigen Sie bei der Anpassung der erweiterten Einstellungen von Internet Shield die folgenden Faktoren.

Glaubwürdige Schnittstelle

Glaubwürdige Schnittstellen können verwendet werden, wenn der Computer mit installierter F-Secure Internet Security 2003-Anwendung als Netzwerk-Gateway, z. B. bei gemeinsamer Internet-Verbindung unter Windows, agiert. Die für lokale Netzwerke verwendete Netzwerkschnittstelle kann auf **Glaubwürdige Schnittstelle** eingestellt werden, so dass auf diese Schnittstelle keine Internet Shield-Regeln angewendet werden.

Hinweis: Diese Netzwerkschnittstelle wird völlig offen gelassen und ist nicht geschützt.

Paketfilter

Die Paketfilterung bildet die Hauptfunktion von Internet Shield; wenn Sie diese Funktion deaktivieren, ist Internet Shield größtenteils unwirksam gegenüber allen Arten von Netzwerkangriffen.

Anwendungssteuerung

Deaktivieren Sie die Anwendungssteuerung nicht vom Fenster **Erweiterte Einstellungen** aus. Durch Deaktivierung der Anwendungssteuerung wird das Risiko von Software-basierten Angriffen erhöht. Dies sollte deswegen nur zur Fehlerbehebung usw. ausgeführt werden.

Wenn Sie die Anwendungssteuerung deaktivieren möchten, öffnen Sie die Internet Shield-Seite, und ändern Sie den Status der Anwendungssteuerung von *Auffordern* zu *Zulassen und protokollieren* um.

6. Automatische Aktualisierungen

Der automatische Aktualisierungsdienst wird transparent im Hintergrund aktiviert, wenn Sie eine Verbindung zum Internet herstellen, und gewährleistet, dass Sie die aktuellsten Aktualisierungen transparent auf Ihrem Computer erhalten.

Sie können im Bereich der automatischen Aktualisierungen folgende Vorgänge ausführen:

- Klicken Sie auf **Aktivieren** bzw. auf **Deaktivieren**, um automatische Aktualisierungen zu aktivieren bzw. zu deaktivieren.
- Zeigen Sie den Zeitpunkt der letzten bzw. der nächsten Aktualisierungsprüfung an.

  Wenn Sie selbst sicherstellen möchten, dass Sie über die aktuellsten Virendefinitionen verfügen, klicken Sie auf **Jetzt prüfen**. Wenn Ihre Definitionen nicht auf dem neuesten Stand sind, werden die aktuellsten Versionen heruntergeladen.

Hinweis: Wenn Sie ein Modem verwenden bzw. über eine ISDN-Verbindung zum Internet verfügen, muss die Verbindung zum Überprüfen auf Aktualisierungen aktiv sein.

Hinweis für ISDN-Benutzer: Automatische Aktualisierungen sind standardmäßig einmal pro Stunde eingeplant. Das bedeutet, dass einmal pro Stunde eine Internet-Verbindung hergestellt wird, wenn Sie über einen ISDN-Router bzw. ein automatisches Wählgerät verfügen (jede Verbindung ist gebührenpflichtig). Wenn Sie die automatische Wahlfunktion Ihres ISDN-Routers ausschalten möchten, deaktivieren Sie die automatischen Aktualisierungen und suchen Sie mit Hilfe der Schaltfläche **Jetzt prüfen** nach Aktualisierungen.

- Prüfen Sie, wann die drei unten stehenden Optionen aktualisiert wurden.

Virendefinitionen	Häufig aktualisierte Virenschutz-Datenbank. Diese automatischen Aktualisierungen werden transparent im Hintergrund ausgeführt, ohne dass Sie dabei aktiv werden müssen, und werden bei jeder Verbindung mit dem Internet aktiviert.
Sicherheitsprofile	Verschiedene Stufen der Sicherheitseinstellungen. Profile werden zur Schutzmaximierung Ihres Computer aktualisiert, sobald neue Angriffsarten entdeckt werden.
Software	Software-Aktualisierungen von F-Secure Internet Security 2003, die im Hintergrund heruntergeladen werden.

7. Meine Anmeldung

Die Seite **Meine Anmeldung** zeigt Informationen zur eigenen Anmeldung an.

Auf der Seite **Meine Anmeldung** stehen Ihnen folgende Optionen zur Verfügung:

- Anzeigen des Anmeldestatus. Das Ablaufdatum Ihrer Anmeldung wird zusammen mit dem aktuellen Status sowie eins der folgenden Statussymbole angegeben:

	Gültig	Ihre Anmeldung ist gültig.
	Läuft bald ab	Ihre Anmeldung ist gültig, läuft aber bald ab.
	Abgelaufen	Ihre Anmeldung ist abgelaufen.

- Online-Verlängerung Ihrer Anmeldung (oder erwerben Sie bei Verwendung einer Testversion eine neue Anmeldung).
- Ändern Ihrer Anmeldenummer.

8. So schützt F-Secure Internet Security 2003 Ihren Computer

8.1 Virenschutz

Programme oder Dateien wie beispielsweise Viren, Würmer, Trojanische Pferde, Jokes und Fehlmeldungen, die entwickelt werden, um auf Ihrem Computer Schaden anzurichten, werden als Malware (abgeleitet von „malicious software“) bezeichnet.

Der Virenschutz entdeckt und entfernt Viren und andere bösartige Computerprogramme von Ihrem Computer. Der Virenschutz von F-Secure Internet Security 2003 prüft geöffnete Dateien bei jedem Öffnen von der Festplatte, einem externen Speichermedium oder dem Internet auf Viren.

Aktuellste Virenschutzsoftware und automatisch aktualisierte Virusdefinitionen bieten Ihnen den besten Schutz gegen Viren. Das Forschungslabor von F-Secure Anti-Virus veröffentlicht und aktualisiert regelmäßig Virusdefinitionen, Profile und die F-Secure Internet Security 2003-Software, die bei jeder Verbindung mit dem Internet schnell und automatisch von F-Secure Internet Security 2003 heruntergeladen werden.

Der Virenschutz von F-Secure verwendet mehrere Virus-Scanmodule, um lückenlosen Schutz gegen Viren zu gewährleisten. Von diesen schützt besonders das Modul für heuristisches Scannen gegen neue und unbekannte Viren.

8.2 Internet Shield

Bei jeder Verbindung, die Ihr Computer zum Internet herstellt, ist er ein mögliches Ziel für Internetangriffe aus unbekannten Quellen. In einigen Fällen sind dies jedoch keine wirklichen Angriffe, sondern harmlose Meldungen, die versehentlich bei Ihrem Computer eingehen. Es kann in anderen Fällen allerdings auch vorkommen, dass ein unbekannter Dritter oder Computer vorsätzlich versucht, auf Ihren Computer und Ihre Dateien zuzugreifen.

Sicherheitslücken für Ihren Computer ergeben sich auf vielfache Weise, wie beispielsweise durch Folgendes:

- Versehentlich offen gelassene Dienstprogramme können von Dritten problemlos gefunden und missbraucht werden.

Internet Shield schützt Ihren Computer bei Verbindungen zum Internet. Er lässt nur die Verbindungen für Ihren Computer zu, die im ausgewählten Profil zugelassen sind. Datenverkehr über andere als diese Verbindungen wird verhindert, so dass Hacker nahezu keine Chance haben, die Informationen auf Ihrem Computer einzusehen oder zu manipulieren.

- Ihr Computer überträgt Informationen über sein System. Wenn Sie eine Internetverbindung hergestellt haben, kann jeder, der sich damit auskennt, diese Informationen als Grundlage für einen Angriff gegen Sie verwenden.

Internet Shield verhindert, dass Ihr Computer im Internet Systeminformationen sendet, und sorgt dafür, dass keine Informationen über Sie oder Ihren Computer über ausgehende Verbindungen freigegeben werden.

- Einige Trojanische Pferde verstecken sich in Software, der Sie normalerweise vertrauen. Sie nutzen eine Verbindung oder Anwendung, die Sie für sicher halten, um Daten über Sie oder Ihren Computer zu übertragen.

Internet Shield erkennt Datenübertragungsversuche von Trojanischen Pferden und verhindert das Herstellen der Verbindung, so dass Ihre Daten jederzeit gegen unerwünschte Angriffe geschützt sind.

8.3 So schützen Sie sich gegen Viren und andere Malware

F-Secure Internet Security 2003 bietet den besten Schutz gegen Viren, da es bekannte Viren bereits unschädlich macht, bevor sie den Computer infizieren können. Zum Schutz Ihres Computers können Sie jedoch auch durch Folgendes beitragen:

- Halten Sie Ihr Betriebssystem und Ihre Anwendungen auf dem neuesten Stand, und wenden Sie aktuelle Patches an, sobald diese verfügbar sind. Beziehen Sie Aktualisierungen immer direkt vom Händler.
- Speichern Sie heruntergeladene Dateien immer zuerst auf Ihrer Festplatte, bevor Sie sie öffnen oder ausführen. Durch das Speichern von heruntergeladenen Dateien wird gewährleistet, dass F-Secure Internet Security 2003 diese überprüft.
- Die meisten Würmer nutzen E-Mails zur Ausbreitung und sind auf Benutzer von Microsoft Outlook oder Outlook Express ausgerichtet. Wenn Sie eine Outlook-Version verwenden müssen, laden Sie sich regelmäßig den aktuellsten Sicherheits-Patch für Microsoft Outlook herunter, und installieren Sie diesen auf Ihrem System.
- Wenn Sie E-Mail-Werbung oder unerbetene E-Mails erhalten oder eine von einem Freund oder Bekannten erhaltene E-Mail merkwürdig scheint, öffnen Sie die Anhänge nicht bzw. klicken Sie

nicht auf die enthaltenen Web-Links. Wenn Sie einen Anhang öffnen möchten, speichern Sie diesen auf Ihrer Festplatte, und öffnen Sie ihn von dort aus. Dadurch wird gewährleistet, dass F-Secure Internet Security 2003 den Anhang auf Viren überprüft.

- Vermeiden Sie Dateien von öffentlichen Newsgroups und Online-Chat-Systemen wie beispielsweise IRC oder ICQ.
- Leiten Sie keine Virenwarnungen oder Kettenbriefe weiter, die Sie von anderen Absendern erhalten.

Installation

F: Installation fehlgeschlagen. Was ist geschehen?

A: Wenn keine Internetverbindung hergestellt wurde, konnte F-Secure Internet Security 2003 Ihre Anmeldung nicht überprüfen. Prüfen Sie, dass eine Internetverbindung vorhanden ist, und installieren Sie F-Secure Internet Security 2003 erneut.

Allgemeine Verwendung

F: F-Secure Internet Security 2003 ist sehr langsam bzw. kann nicht geöffnet werden. Wo liegt der Fehler?

A: Internet Explorer 3.0 oder höher ist unter Umständen nicht installiert. Überprüfen Sie, welche Version von Internet Explorer installiert ist (Internet Explorer ist über die Website der Microsoft Corporation erhältlich).

F: Das Symbol für F-Secure Internet Security 2003 wird nicht in der Systemleiste in der unteren rechten Ecke des Bildschirms angezeigt.

A: Unter Windows XP können Symbole ausgeblendet werden. Um ausgeblendete Symbole anzuzeigen, klicken Sie auf die Schaltfläche  . Wenn Sie nicht Windows XP verwenden, installieren Sie F-Secure Internet Security 2003.

Virenschutz

F: F-Secure Internet Security 2003 kann eine infizierte Datei auf dem Computer nicht desinfizieren, löschen oder umbenennen. Was soll ich tun?

A: Siehe *„Viren nach Fehlschlagen des Desinfektions-Assistenten entfernen“* auf Seite 116.

Internet Shield

F: Ich habe den Verdacht, über das Internet von einem Hacker angegriffen zu werden. Was soll ich tun?

A: Rufen Sie die Internet Shield-Seite auf, und wählen Sie das Profil **Alle blockieren** aus. Weitere Informationen zum Auswählen eines Internet Shield-Profils finden Sie unter *„Ändern Ihres Internet Shield-Profils“* auf Seite 122.

Anwendungssteuerung

F: Wie kann ich die Berechtigungen der Anwendung für Internetverbindungen ändern? Wie kann ich für eine Anwendung, für die dies bisher untersagt war, Internetverbindungen zulassen?

A: Siehe *„Ändern der Verbindungsrechte von Anwendungen“* auf Seite 122.

F: Mein E-Mail-Programm (bzw. ein anderes Programm wie beispielsweise der Internet-Browser) funktioniert nicht mehr.

A: Sie haben unter Umständen versehentlich eingestellt, dass das Programm keine Verbindungen herstellen darf. Weitere Informationen zum Zulassen von Verbindungen finden Sie unter *„Ändern der Verbindungsrechte von Anwendungen“* auf Seite 122.

F: Für welche Programme bzw. Anwendungen können Verbindungen zum Internet zugelassen werden?

A: Weitere Informationen zur Bestimmung, für welche Anwendungen Verbindungen verhindert oder zugelassen werden sollen, finden Sie unter *„Verwendung der Anwendungssteuerung“* auf Seite 122.

Automatische Aktualisierungen

F: Was passiert, wenn mein Computer bei Fälligkeit einer automatischen Virus-Aktualisierung offline ist?

A: Wenn Sie das nächste Mal online sind, lädt F-Secure Internet Security 2003 die aktuellste automatische Virus-Aktualisierung herunter.

F: Wie oft sollte die Virusdefinitionsdatenbank aktualisiert werden?

A: Virusdefinitionsdatenbanken werden automatisch aktualisiert, wenn die Funktion zur automatischen Aktualisierung aktiviert ist. Wenn Sie die Datenbanken manuell aktualisieren möchten, sollten Sie dies mindestens einmal wöchentlich vornehmen.

F: Ich versuche, manuell nach Virusdefinitionsdatenbank-Aktualisierungen zu suchen (durch Klicken auf „Jetzt prüfen“), aber nichts passiert.

A: Wenn Sie ein Modem verwenden oder über einen ISDN-Anschluss verfügen, müssen Sie vor dem Klicken auf **Jetzt prüfen** manuell eine Verbindung zum Internet herstellen.

Meine Anmeldung

F: Bei der Installation von Software zeigt der Virenschutz eine Meldung an, dass diese einen Virus enthält, und der Installationsvorgang kann aus diesem Grund nicht abgeschlossen werden.

A: Wenn Sie sicher sind, dass die Software keine Viren enthält, können Sie einen der folgenden Schritte ausführen:

- Wählen Sie ein weniger strenges Virenschutzprofil aus (Anweisungen dazu finden Sie unter *„Virenschutzprofile ändern“* auf Seite 112), oder
- klicken Sie mit der rechten Maustaste auf das Symbol in der Systemleiste (in der rechten unteren Ecke des Bildschirms), und wählen Sie *F-Secure-Produkte entladen* aus. Denken Sie daran, die Produkte nach Abschluss der Installation wieder zu laden.

Glossar

Anwendung

Ein für einen bestimmten Zweck geschriebenes Software-Programm. Anwendungen sind in der Regel manuell zu starten.

Anwendungssteuerung

Die Anwendungssteuerung ist eine Funktion in F-Secure Internet Security 2003, mit der automatisch eine Anwendung, die von Ihrem Computer aus mit dem Internet verbunden ist, geprüft wird, indem die Anwendung mit der Liste von sicheren (bereits genehmigten) Software-Programmen und bereits als schädlich bekannten Software-Programmen (Trojaner usw.) verglichen wird.

„Denial of Service“-Angriffe

Ein expliziter Angriffsversuch, bei dem berechtigte Benutzer durch Unterbrechung der Verbindungen, Überlastung eines Netzwerks oder Unterbinden des Netzwerkzugriffs einzelner Personen an der Verwendung eines Dienstes gehindert werden.

DNS

Im Domänennamensystem (DNS) sind die Namen der Internet-Domäne enthalten und in Internet-Protokolladressen übersetzt. Ein Domänenname ist eine aussagekräftige, leicht merkbare Beschreibung für eine Internet-Adresse. Die Internet-Adresse www.some.domain.org ist beispielsweise ein DNS-Name.

Heuristisch

Untersuchende Problemlösung, bei der selbstlernende Techniken angewandt werden.

Schädliche Programme

Schädliche Programme, so genannte „Malware“, sind Programme oder Dateien, die allein dazu entwickelt wurden, auf Ihrem Computer Schaden anzurichten. Dazu gehören Computerviren, Würmer und Trojanische Pferde.

Paket

Ein Paket ist eine Dateneinheit, die von einer Quelle zu einem Ziel im Internet gesendet wird. Wenn Dateien (z. B. eine E-Mail) im Internet von einer Adresse zur anderen gesendet werden, werden diese in zum Weiterleiten passende Pakete aufgeteilt. Wenn sie ihren Adressaten erreicht haben, werden sie wieder zur ursprünglichen Datei zusammengesetzt.

Profil

Profile sind im voraus konfigurierte Attribute, mit denen Ihre Sicherheitsstufe festgelegt wird. Sie werden automatisch aktualisiert, damit Sie jederzeit gegen neue Arten bösartiger Computerprogramme und Internetangriffe geschützt sind.

Teilnetz

Dieser Begriff steht für „Teilnetzwerk, d. h. bildet einen Abschnitt eines Netzwerks. Computer mit demselben Teilnetz sind sich in der Regel physisch nahe und verfügen über IP-Adressen, deren ersten beiden oder drei Ziffer identisch sind.

Trojanisches Pferd

Ein Programm, das absichtlich Aktionen durchführt, die der Benutzer des Programms nicht erwartet.

Virus

Ein Computerprogramm, das sich durch eigene Reproduktion verbreitet.

Virendefinitionsdatenbank

Mit Virendefinitions-Datenbanken werden Viren entdeckt. Wenn ein neuer Virus entdeckt wird, müssen die Datenbanken aktualisiert werden, damit der Virenschutz diesen Virus ermitteln kann.

Wurm

Ein Computerprogramm, das sich selbst durch Einfügen eigener Kopien in Netzwerkcomputern vermehren kann.

Kundendienst und Wartung

Technischen Telefon-Support innerhalb Deutschlands erhalten Sie unter folgender Rufnummer:

0190 - 88 44 33*

* 1,86 EUR/Minute innerhalb des deutschen Festnetzes

Technischen EMail-Support (kostenlos) erhalten Sie über das Support Center unseres Partners Softline AG: support@softline.de

Sollten außerhalb des Technischen Supports noch Fragen offen sein, so steht Ihnen der WSKA Verlag gerne zur Verfügung.

WSKA Verlag GmbH

Goldgasse 34

77652 Offenburg - Germany

Telefon +49 - 1 80 - 5 97 52 00

Telefax +49 - 1 80 - 5 97 52 01

Email: Vertrieb@wska.com

Web: www.wska.com