

# F-Secure Mobile Security

for Series 80

User's Guide



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

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

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

GB2353372 GB2366691 GB2366692 GB2366693 GB2367933 GB2368233  
GB2374260

# Contents

<b>About This Guide</b>	<b>1</b>
How This Guide Is Organized .....	2
Conventions Used in F-Secure Guides .....	3
<b>Chapter 1 Introduction</b>	<b>5</b>
1.1 F-Secure Mobile Security .....	6
1.2 Key Features .....	6
<b>Chapter 2 Installation</b>	<b>7</b>
2.1 System Requirements .....	8
2.2 Installing F-Secure Mobile Security .....	8
2.2.1 Activating The Update Service .....	9
2.3 Uninstalling F-Secure Mobile Security .....	10
<b>Chapter 3 Using F-Secure Mobile Security</b>	<b>11</b>
3.1 Overview .....	12
3.2 Starting F-Secure Mobile Security .....	12
3.3 Main View .....	13
3.4 Selecting the Virus Protection .....	14
3.4.1 Real-time Scanning .....	15
3.4.2 Manual Scanning .....	15
3.5 Processing Infected Files .....	17
3.5.1 Infections List .....	17

3.6	Keeping F-Secure Mobile Security Up-To-Date .....	19
3.6.1	Update Settings .....	19
3.6.2	Upgrading the Application .....	20
3.6.3	Purchasing Subscription Service Time .....	21
3.7	Firewall .....	22
3.7.1	Protection Levels .....	22
<b>Chapter 4</b>	<b>Troubleshooting</b>	<b>26</b>
4.1	Updates .....	27
4.2	Subscription .....	29
4.3	Firewall .....	29
4.4	Uninstallation .....	30
<b>Chapter 5</b>	<b>Technical Support</b>	<b>31</b>
5.1	Overview .....	32
5.2	Web Club .....	32
5.3	Virus Descriptions on the Web .....	32
5.4	Electronic Mail Support .....	32
	<b>About F-Secure Corporation</b>	

# ABOUT THIS GUIDE

How This Guide Is Organized.....	2
Conventions Used in F-Secure Guides .....	3

## How This Guide Is Organized

F-Secure Mobile Security User's Guide is divided into the following chapters:

**Chapter 1. Introduction.** Provides general information about F-Secure Mobile Security.

**Chapter 2. Installation.** Gives instructions on installing and setting up F-Secure Mobile Security.

**Chapter 3. Using F-Secure Mobile Security.** Describes how to use F-Secure Mobile Security.

**Chapter 4. Troubleshooting.** Provides solutions to common problems.

**Chapter 5. Technical Support.** Provides the contact information for assistance.

**About F-Secure Corporation.** Describes the company background and products.

## Conventions Used in F-Secure Guides

This section describes the symbols, fonts, and terminology used in this manual.

### Symbols



**WARNING:** The warning symbol indicates a situation with a risk of irreversible destruction to data.



**IMPORTANT:** An exclamation mark provides important information that you need to consider.



**REFERENCE** - A book refers you to related information on the topic available in another document.



**NOTE** - A note provides additional information that you should consider.



**TIP** - A tip provides information that can help you perform a task more quickly or easily.

⇒ An arrow indicates a one-step procedure.

### Fonts

**Arial bold (blue)** is used to refer to menu names and commands, to buttons and other items in a dialog box.

*Arial Italics (blue)* is used to refer to other chapters in the manual, book titles, and titles of other manuals.

*Arial Italics (black)* is used for file and folder names, for figure and table captions, and for directory tree names.

Courier New is used for messages on your computer screen.

**Courier New bold** is used for information that you must type.

**SMALL CAPS (BLACK)** is used for a key or key combination on your keyboard.

[Arial underlined \(blue\)](#) is used for user interface links.

Times New Roman regular is used for window and dialog box names.

## PDF Document

This manual is provided in PDF (Portable Document Format). The PDF document can be used for online viewing and printing using Adobe® Acrobat® Reader. When printing the manual, please print the entire manual, including the copyright and disclaimer statements.

## For More Information

Visit F-Secure at <http://www.f-secure.com> for documentation, training courses, downloads, and service and support contacts.

If you have any questions, comments, or suggestions about this or any other F-Secure document, please contact us at [documentation@f-secure.com](mailto:documentation@f-secure.com).

# 1

## INTRODUCTION

F-Secure Mobile Security .....	6
Key Features .....	6

## 1.1 F-Secure Mobile Security

F-Secure Mobile Security is a software product that protects data stored in your device against malicious code attacks.

F-Secure Mobile Security scans all files for viruses automatically when they are accessed. All infected files are immediately quarantined to protect all other data on the device. The automatic scanning happens transparently in the background.

To work effectively, antivirus software requires an always up-to-date virus definition database. F-Secure Mobile Security gets the latest virus definition databases automatically.

## 1.2 Key Features

F-Secure Mobile Security offers the following key features.

### Transparent Operation

The application runs in the background while you use your device.

### Extensive scanning

The application automatically scans all files when they are accessed. You can also manually scan your device for viruses whenever you want.

### Automatic updates

The application automatically downloads regular updates to keep the virus definition database up-to-date.

### Firewall

The application protects you from potential network harm by blocking information that does not meet the set security criteria.

# 2

## INSTALLATION

System Requirements .....	8
Installing F-Secure Mobile Security .....	8
Uninstalling F-Secure Mobile Security.....	10

## 2.1 System Requirements

To use F-Secure Mobile Security, your device must meet the following requirements:

Device:	Nokia Series 80 devices (Nokia 9300 and Nokia 9500)
Available memory:	400 KB

## 2.2 Installing F-Secure Mobile Security



**IMPORTANT:** *F-Secure Mobile Security cannot be installed on a memory card.*

To install F-Secure Mobile Security:

1. Open the inbox and scroll to the message that contains the installation package.



*For more information, refer to the User's Guide that came with your device.*

2. Open the message, and press **Yes** to confirm the installation.
3. Read the License agreement, and press **Ok**.
4. Wait until the installation is complete.
5. Enter your subscription number when prompted.



*Your subscription cannot be authenticated if you have tried to transfer the F-Secure Mobile Security service subscription onto another device more than four times.*

6. Press **Yes** to update the virus definition database.

7. F-Secure Mobile Security retrieves the latest virus definition database update from the Internet. For more information, see “[Keeping F-Secure Mobile Security Up-To-Date](#)”, 19.



**IMPORTANT:** *F-Secure Mobile Security cannot detect the latest viruses with an outdated database. You must keep the virus definition database up-to-date.*

## 2.2.1 Activating The Update Service

Before you can use F-Secure Mobile Security, you have to activate the update service with the activation code.

If you have given your mobile phone number to your retailer, you will receive the activation message as an SMS message. If you do not receive it, enter your subscription number when you start the F-Secure Mobile Security for the first time. To activate the update service later, press **Activate** in the main view.



*If you do not know your subscription number, contact your service provider or retailer.*

### Trial version

If you want a trial version of F-Secure Mobile Security, select *30 days evaluation*. To continue using it after the 30-day trial period, see “[Purchasing Subscription Service Time](#)”, 21.

## 2.3 Uninstalling F-Secure Mobile Security



**IMPORTANT:** Remove all quarantined and infected files from your device before you uninstall F-Secure Mobile Security.

### To uninstall F-Secure Mobile Security:

1. Open F-Secure Mobile Security.
2. Open *Tools menu* and select *Uninstall Mobile Security*.
3. Press **Uninstall** to confirm the uninstallation.

# 3

## USING F-SECURE MOBILE SECURITY

Overview.....	12
Starting F-Secure Mobile Security.....	12
Main View.....	13
Selecting the Virus Protection.....	14
Processing Infected Files.....	17
Keeping F-Secure Mobile Security Up-To-Date.....	19
Firewall.....	22

## 3.1 Overview

F-Secure Mobile Security scans all accessed and modified data on your device automatically for malicious content when the real-time scanning is enabled. If you do not want to use the real-time scanning, you can manually scan all the data for viruses whenever you want.

When F-Secure Mobile Security detects an infected file, you can delete or quarantine it. If you delete the file, it is removed completely while the quarantined file is locked up so that it cannot be accessed.

## 3.2 Starting F-Secure Mobile Security

To open F-Secure Mobile Security, select the Security icon in *Desk* and press **Open**.



*When the real-time scanning mode is selected, F-Secure Mobile Security runs in the background automatically. For more information, see “[Real-time Scanning](#)”, 15.*

## 3.3 Main View

The F-Secure Mobile Security main view opens when you start the application.

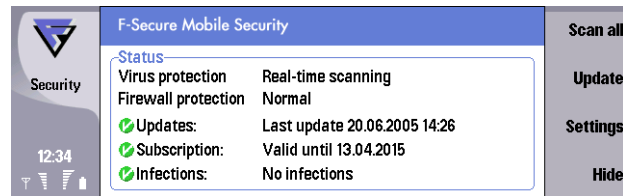


Figure 3-1 Main view in F-Secure Mobile Security

The main view displays the virus protection and firewall settings, and the product status. For more information about *Virus protection*, see “[Selecting the Virus Protection](#)”, 14.

Virus protection	Displays the type of virus scan in use. For more information, see “ <a href="#">Selecting the Virus Protection</a> ”, 14.
Firewall protection	Displays the firewall protection level.
Updates	Displays the date when you received the last update. For more information, see “ <a href="#">Update Settings</a> ”, 19.
Subscription	Displays the subscription status. You should renew your license before it expires. For more information, see “ <a href="#">Purchasing Subscription Service Time</a> ”, 21, or contact your retailer.
Infections	Displays the number of infected files that have been found.

Press **Scan all** to scan all files on your device and on the inserted memory card for viruses. For more information, see “[Running A Manual Scan](#)”, 15.

Press **Update** to get the latest virus definition database update. For more information, see “[Keeping F-Secure Mobile Security Up-To-Date](#)”, 19.

## Closing the Main View

Press **Settings** to change the protection and automatic update settings.

Select **File menu**→**Hide Mobile Security**, or press **Hide** to close the main view. If you have selected real-time scanning, F-Secure Mobile Security keeps running in the background.

To shut down F-Secure Mobile Security completely, select **File menu**→**Exit**.



**IMPORTANT:** *If you shut down the application, the infected files are not quarantined, and the system is not protected against viruses.*

## 3.4 Selecting the Virus Protection

You can set F-Secure Mobile Security to scan all files for viruses automatically when they are accessed, or you can scan files for viruses manually.

To change the scanning type:

1. Press **Settings** in the main view.
2. Select *Virus Protection*, then select one of the following:
  - › *Real-time* - F-Secure Mobile Security runs in the background and scans files when they are accessed or modified. All infected files are quarantined automatically. For more information, see "*Real-time Scanning*", 15.
  - › *Manual Scan* - F-Secure Mobile Security scans files only when you run the virus scan yourself. For more information, see "*Manual Scanning*", 15.



**IMPORTANT:** *If you do not select real-time scanning, you should manually scan your device each time you transfer new data to it.*

3. Press **Done** to accept the settings.

### 3.4.1 Real-time Scanning

The real-time scan scans files for malicious content automatically when files are accessed or modified.

Real-time scanning runs in the background, and when it detects a virus, it is immediately quarantined and added to the Infections list. For more information, see “[Infections List](#)”, 17.

#### Virus alerts

When F-Secure Mobile Security detects a virus during a real-time scan, it displays the following warning:

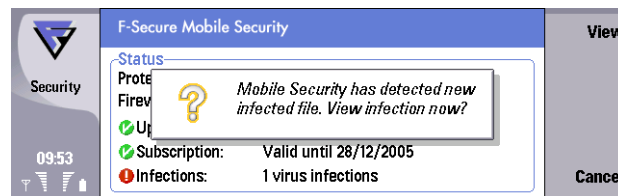


Figure 3-2 Virus alert in F-Secure Mobile Security

Press **View** to view a list of all infected files. For more information, see “[Infections List](#)”, 17.

### 3.4.2 Manual Scanning

With manual scanning, you can scan your device and the inserted memory card.

#### Running A Manual Scan

To manually scan your device and the inserted memory card:

1. Press **Scan all** to start the manual scan.  
You can press **Cancel** to stop the scan at any time.
2. After the virus scan is finished, the application displays the following information:

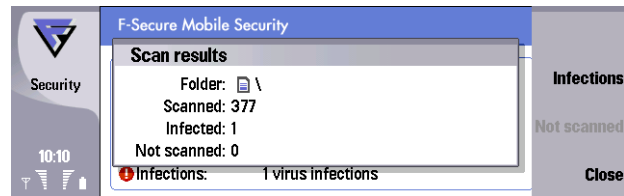


Figure 3-3 Virus scan results in F-Secure Mobile Security

**Scanned**                      The number of files that were scanned.

**Infected**                      The number of infections found. Press **Infections** to view a list of infected files.

For more information about removing infected files, see *"Processing Infected Files", 17*.

**Not Scanned**                The number of files that were not scanned. A file cannot be scanned if another program is using the file during the scan.

Press **Not scanned** to view a list of files that could not be scanned. Select the file from the list and press **Details** to view why it could not be scanned.

Press **Close** to exit the scan. All infected files are quarantined and cannot be accessed when F-Secure Mobile Security is running in the background.

## 3.5 Processing Infected Files

When F-Secure Mobile Security finds a virus in a file, you can remove the infected file completely, or lock it up so that the infected file cannot be accessed.

### 3.5.1 Infections List

The *Infections* list is opened automatically if F-Secure Mobile Security detects any infections during the scan. The *Infections* list displays all detected infected files in the device.

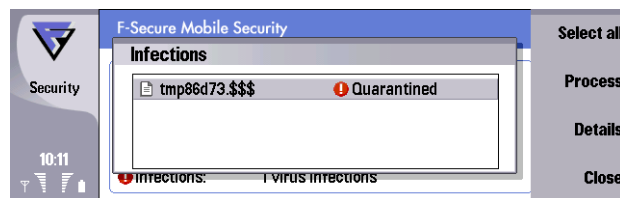


Figure 3-4 Infections list in F-Secure Mobile Security

The list displays the name of the infected file and the current infection status.

- › A *Quarantined* file is locked and cannot be accessed.
- › A *Released* file is infected but is not quarantined.

Select the infected files, and press **Process** to choose one of the following actions:

- › **Quarantine** - Quarantine the infected file. Quarantined files cannot be accessed when F-Secure Mobile Security is running in the background.
- › **Delete** - Delete the infected file. Deleted files are removed completely. To restore the deleted file, reinstall it or restore it from the backup copy.
- › **Release** - Release the quarantined file. If you release the file, you can access it and use it, but at your own risk.

Press **Details** to view more details about the selected file. The *Infection details* view displays the path and file name of the infected file, and the name of the virus that has infected the file.



You can find in-depth virus descriptions in the F-Secure web site:  
<http://www.f-secure.com/virus-info/>.


Press **Close** to close the *Infections* list and return to the main view.

## 3.6 Keeping F-Secure Mobile Security Up-To-Date

You can keep F-Secure Mobile Security up to date by downloading the latest virus definition database from the update service.


The virus definition database contains information about all the viruses that the application can find during the scan. An up-to-date virus definition database gives you the best possible protection.

You must have an active connection to the Internet for F-Secure Mobile Security to check for updates.

 *Your copy of F-Secure Mobile Security includes a license. During this time, you can freely update your F-Secure Mobile Security. When your license expires, you can update your copy only after renewing your license.*


### 3.6.1 Update Settings

You can get F-Secure Mobile Security updates automatically every time you open a connection to the Internet or manually whenever you want.

 *If the update service has not been activated, you cannot receive any updates. Press **Activate** to activate the update service. For more information, see “[Activating The Update Service](#)”, 9.*

### Automatic Updates

You can set F-Secure Mobile Security to download updates automatically once a day when the device has an active connection to the Internet.

 *F-Secure Mobile Security does not open a connection, but it recognizes a connection being opened by, for example, a Web browser.*

To select automatic updates:

1. Press **Settings**.
2. Change *Automatic Updates* to **Enabled**.

3. Press **Done** to exit the settings.



**IMPORTANT:** *Automatic Updates can be selected only if real-time scanning is on.*

If you have selected real-time scanning, F-Secure Mobile Security detects open internet connections. F-Secure Mobile Security downloads the virus definition database update automatically if more than 24 hours have passed since the last update.

It is recommended that you scan your device for viruses after you receive a new virus definition database update

## Manual Updates

To update F-Secure Mobile Security manually:

1. Press **Update**.
2. Select the Internet access point to connect to the update server. F-Secure Mobile Security connects to the update server and downloads the latest virus definition database. The application takes the virus definition database update into use immediately.



*For more information, see the User Guide of your device.*

3. When the update is complete, press **OK** to scan your device for viruses. For more information on scanning, see “[Running A Manual Scan](#)”, 15.

## 3.6.2 Upgrading the Application

When a new F-Secure Mobile Security version is available, F-Secure Mobile Security prompts you to download the software update.



Figure 3-5 Upgrading F-Secure Mobile Security

Press **Yes** to get the latest version of F-Secure Mobile Security. If the updated virus definition database requires a software update to work properly, the upgrade is downloaded automatically.

The new version is installed automatically.

### 3.6.3 Purchasing Subscription Service Time

To keep your device continuously protected, you should purchase additional service time well before the expiration date. The additional service time purchased is either added to the time remaining in your previous order or to your free evaluation period.

#### To purchase more service subscription time through your PC browser:

1. Open <http://www.f-secure.com/estore/> in the web browser with the PC computer.
2. Enter your subscription number in the *Subscription Number* field to identify your subscription.



*F-Secure eStore accepts the most commonly used credit cards and wire/bank transfers.*

3. Follow the instructions on the screen.

## 3.7 Firewall

The firewall in F-Secure Mobile Security works quietly in the background. It monitors incoming and outgoing Internet and network information, and protects you from intrusion attempts.

The firewall protection level has been set to *Normal*. This level gives you good protection and does not affect using the most common applications.

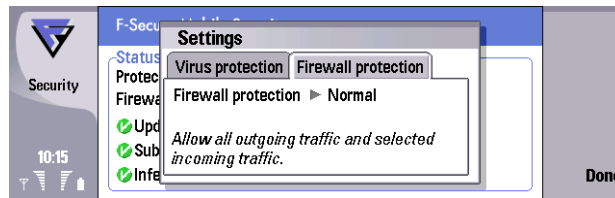


Figure 3-6 Firewall Settings with Normal protection level.

### 3.7.1 Protection Levels

The firewall has five protection levels:

Level	Description	Protection
Allow All	Allows all network traffic. Does not stop any incoming or outgoing connections.	No protection.
Normal	Allows all outgoing connections and does not stop preinstalled applications. Recommended level.	Good protection.

High	Allows preinstalled applications to connect, but may stop rarely used applications.	High protection
Deny All	Stops all network traffic. You cannot use your e-mail, MMS or web services.	Total protection.
Custom	Allows preinstalled applications to connect, but may stop rarely used applications. You can add three types of rules: <i>Normal</i> , <i>Trigger</i> , <i>Custom</i> (see “ <a href="#">Custom Level Rules</a> ”, 23).	High protection

## Custom Level Rules

The *Custom* protection level has three types of rules you can add:

Rule	Description
<i>Normal</i>	To allow TCP or UDP ports in or out.
<i>Trigger</i>	For more complex connections. You need to set an “if - then” structure to define a protocol and ports that trig a rule on for another protocol and port.
<i>Custom</i>	To define a protocol number that is allowed in and out.

### **Add a Normal rule**

You need to specify the following:

- › *Rule name* - define the rule name
- › *Rule Type* - Normal
- › *Protocol* - TCP or UDP
- › *Direction* - incoming or outgoing
- › *Ports* - set the destination port range (from 1 to 65535)

### **Add a Trigger rule**

You need to specify the following:

- › *Rule name* - define the rule name
- › *Rule Type* - Trigger
- › Define the rule under *If connection exists*: that trigs the rule defined under *Then allow connection to*:

### **Add a Custom rule**

You need to specify the following:

- › *Rule name* - define the rule name
- › *Rule Type* - Custom
- › *Protocol number* - set a protocol number between 0 to 255.

## Terminology

- Connection** A connection is made every time information is sent between two devices. When a device wants to make a connection to another, it has to create, or open, a port so that it can listen to the response.
- IP protocol** The Internet uses Internet Protocol (IP) packets to deliver information from one device to another. IP packets include other protocols, which are designed for different kinds of tasks.
- Port** A port is an address inside a protocol where information can be sent, or an address that an Internet server can listen to.
- Protocol** Protocols are the agreed form for how information is sent between two devices. Different protocols are used for sending different kinds of information. The devices must support the same protocols to be able to communicate.
- Rule** A rule is an instruction for the firewall to restrict incoming and/or outgoing information. A simple rule can be the following: "allow outgoing TCP packets to port 80, any address". This means that the firewall allows all information to and from port 80.

TCP, TCP/IP protocol

The Transmission Control Protocol (TCP) makes it possible for two devices to make a connection and exchange information. TCP guarantees that the information is delivered in exactly the same form it was sent. TCP is often referred to as TCP/IP.

UDP protocol

User Datagram Protocol (UDP) is used for sending audio or video information on IP networks.

# 4

## TROUBLESHOOTING

Updates .....	27
Subscription.....	29
Firewall .....	29
Uninstallation.....	30

## 4.1 Updates

**Q. When trying to connect to the update server, I get a notification that no Internet access points are configured. What causes this?**

A. You may have deleted the Internet access point that you selected during the activation. With no defined Internet access point, the application cannot check for updates. Go to the Update settings view and select one of the Internet access points or create a new one.

**Q. I have defined an Internet access point, but I am unable to get the updates. What can I do?**

A. Check the Internet access point settings with your operator. You should also check that the date and time settings in your device are correct. If you have problems connecting through WAP access points, you should connect through the Internet.



*The Internet access point settings are operator specific.*

**Q. I get a notification that the update service cannot authenticate my device. Why?**

A. This error message is displayed when the update server cannot authenticate the subscription. Reasons for the authentication failure can be as follows:

- › The F-Secure F-Secure Mobile Security installation folder files have been tampered.
- › There have been more than four attempts to move the F-Secure F-Secure Mobile Security installation and service subscription to another device.

**Q. My virus definition database seems to be corrupted. What should I do?**

- A. You should immediately update your virus definition database. After that, in the Scan settings view, first go to the Scan view and change the scanning mode to **Real-time**. Then, go to the Update view and change automatic updates to **Enabled**. Select to *Scan All*.

**Q. How much data traffic automatic updates generate?**

- A. When the Automatic Update feature is enabled and when the connection to the Internet is active, F-Secure Mobile Security checks for updates once a day at most. Depending on the amount of available updates, every checking generates 2-4 KB. For example, if you are connected to the Internet at least once a day, automatic updates generate approximately an extra 100 KB a month. If your GSM operator bills you one euro per 1MB, the automatic updates add approximately 10 cents to your phone bill.

If an updated application is also available, because of the large amount of data, F-Secure Mobile Security displays the amount of data to be downloaded and prompts you for confirmation before starting to download the updated application.

**Q. The application upgrade was interrupted. How can I continue it?**

- A. You cannot cancel the upgrade process. However, if you interrupt it by, for example, removing the battery while new files are being installed, an 'Update AV' message is displayed next time you restart F-Secure Mobile Security. Press **Update F-Secure Security** to resume the upgrade process.

**Q. The application upgrade did not finish because there was not enough storage space. What can I do?**

- A. If there is not enough storage space to complete the application upgrade, F-Secure Mobile Security prompts you either to delete some files before continuing the upgrade process or to cancel the upgrade process and continue it at a later time.

## 4.2 Subscription

**Q. I receive an ‘Invalid subscription number’ error message when I enter my subscription number. What should I do?**

A. You have entered an invalid subscription number. You should check your subscription number and re-enter it.

**Q. What should I do when my subscription is about to expire or has expired?**

A. If your subscription has expired and you want to renew it, press **Yes** to purchase more subscription service time. For more information, see “*Purchasing Subscription Service Time*”, 21.

## 4.3 Firewall

**Q. How can I use IM++ with F-Secure Mobile Security?**

A. IM++ works with *Allow All* and *Normal* protection levels. If you are using *High* protection, you have to make a new rule. The new rule depends on the service provider:

MSN messenger: TCP Outgoing 5050

Jabber: TCP Outgoing 5222

ICQ: TCP Outgoing 5190

AOL: TCP Outgoing 5190

**Q. How can I test that the firewall is working?**

A. Go to the *Firewall Protection* settings and select *Deny All* as the protection level. The *Deny All* protection level closes all connections to and from the Internet, and you will get a failed connection error message. Remember to change the protection level back to *Normal* after the test.

## 4.4 Uninstallation

- Q. I can't uninstall F-Secure Mobile Security, what should I do?**
- A. Check that you don't have an active or open connection through the firewall; close all connections and try again.

# 5

## TECHNICAL SUPPORT

Overview.....	32
Web Club.....	32
Virus Descriptions on the Web .....	32
Electronic Mail Support.....	32

## 5.1 Overview

F-Secure Technical Support is available by e-mail and from our Web site. You can access our Web site from within F-Secure Mobile Security or from your Web browser.

For Technical Support of all F-Secure products, go to F-Secure Support Center at: <http://support.f-secure.com/enu/home/>.

## 5.2 Web Club

The F-Secure Web Club provides assistance to the users of F-Secure products. To connect to the Web Club on our Web site, open the Web Club page, and click Web Club on the Web Club tab of the General property page.

To connect to the Web Club directly from within your Web browser, go to <http://www.f-secure.com/webclub/>.

## 5.3 Virus Descriptions on the Web

F-Secure Corporation maintains a comprehensive collection of virus-related information on its Web site. To view the Virus Information Database, connect to: <http://www.F-Secure.com/virus-info/>.

## 5.4 Electronic Mail Support

If you have questions about F-Secure Mobile Security not covered in the manual or online services at <http://www.F-Secure.com/>, you can contact your local F-Secure distributor or F-Secure Corporation directly.

For technical assistance, please contact your local F-Secure Business Partner. Send your e-mail to: [Anti-Virus-<country>@F-Secure.com](mailto:Anti-Virus-<country>@F-Secure.com)

Example: [Anti-Virus-Norway@F-Secure.com](mailto:Anti-Virus-Norway@F-Secure.com)

If there is no authorized F-Secure Anti-Virus Business Partner in your country, you can request basic technical assistance from:

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

When contacting support, prepare and include the following information in your support request:

- › Name and version number of your F-Secure software program (including the build number, if available).
- › Name and version number of your operating system (including the build number).
- › A detailed description of the problem, including any error messages displayed by the program, and any other details, which could help us duplicate the problem.

When contacting F-Secure support by telephone, please do the following so that we may help you more effectively and save time:

- › have your device at hand, so you can follow instructions given by the support technician, or be prepared to write down instructions.
- › Have your device turned on and (if possible) in the state it was in when the problem occurred.

# About F-Secure Corporation

F-Secure Corporation is the fastest growing publicly listed company in the antivirus and intrusion prevention industry with more than 50% revenue growth in 2004. Founded in 1988, F-Secure has been listed on the Helsinki Stock Exchange since 1999. We have our headquarters in Helsinki, Finland, and offices in USA, France, Germany, Italy, Sweden, the United Kingdom and Japan. F-Secure is supported by service partners, value added resellers and distributors in over 50 countries. F-Secure protection is also available through mobile handset manufacturers such as Nokia and as a service through major Internet Service Providers, such as Deutsche Telekom, France Telecom and Charter Communications. The latest real-time virus threat scenario news are available at the F-Secure Antivirus Research Team weblog at <http://www.f-secure.com/weblog/>.

## Services for Individuals and Businesses

F-Secure services and software protect individuals and businesses against computer viruses and other threats coming through the Internet or mobile networks. Our award-winning solutions include antivirus and desktop firewall with intrusion prevention, antispam and antispymware solutions. Our key strength is our proven speed of response to new threats. For businesses our solutions feature a centrally-managed and well-integrated suite of solutions for workstations and servers alike. Focused partners offer security as a service for companies that do not wish to build in-house security expertise.

Visit our website at <http://www.f-secure.com/products/> to learn more about our products and services.



[www.f-secure.com](http://www.f-secure.com)