

# F-Secure Mobile Security

for S60

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

Copyright © 2004-2008 F-Secure Corporation. All rights reserved.

12000066-6J25

# Contents

<b>About This Guide</b>	<b>1</b>
How This Guide Is Organized .....	2
Conventions Used in F-Secure Guides .....	3
Symbols .....	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 Getting the Product Running on Your Device .....	8
2.2.1 Installation .....	8
2.2.2 Activating the Update Service .....	9
2.3 Transferring Subscription to a New Device .....	10
2.4 Uninstalling .....	11
<b>Chapter 3 Using F-Secure Mobile Security</b>	<b>12</b>
3.1 Opening and Closing the Application .....	13
3.2 Scanning for Viruses .....	14
3.2.1 Selecting the Virus Protection Mode .....	14
3.2.2 Processing Infected Files .....	15
3.3 Using Firewall .....	17

3.3.1	Selecting the Protection Level .....	17
3.3.2	Editing Custom Firewall Rules.....	17
3.4	Keeping the Application Up-to-Date.....	19
3.4.1	Selecting the Update Mode .....	20
3.4.2	Application Updates.....	21
3.5	Purchasing Subscription Service Time .....	21
3.6	Troubleshooting .....	22

## **Technical Support** **25**

Overview .....	26
Virus Descriptions on the Web .....	26
Electronic Mail Support .....	26

## **About F-Secure Corporation**

# 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 activating F-Secure Mobile Security.

***Chapter 3. Using F-Secure Mobile Security.*** Describes the F-Secure Mobile Security user interface.

***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.

Arial underlined (blue) is used for user interface links.

## 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.

In our constant attempts to improve our documentation, we would welcome your feedback. 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 S60 device against malicious code attacks and monitors incoming and outgoing connections and protects the device from network intrusion attempts.

F-Secure Mobile Security scans all files for viruses automatically when they are saved, copied, downloaded, synchronized or otherwise modified. All infected files are immediately quarantined to protect all other data on the device. The automatic scanning happens transparently on the background.

To work effectively, antivirus software requires an always up-to-date virus definition database. F-Secure Mobile Security retrieves 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
Getting the Product Running on Your Device .....	8
Uninstalling .....	11

## 2.1 System Requirements

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

- Platform: Nokia S60 (3rd edition) devices.  
See <http://mobile.f-secure.com/devices/> for a full list of supported devices.
- Internet connection: You must have an Internet connection from your device to activate the application.

To test your Internet access point, browse with your device browser to <https://msp.f-secure.com/web-test/>

If you can access the page, your Internet access point is suitable for activation and updates.

## 2.2 Getting the Product Running on Your Device

Getting your F-Secure Mobile Security running on your device is a two-step process:

1. Install F-Secure Mobile Security. See “*Installation*”, 8.
2. Activate your subscription. See “*Activating the Update Service*”, 9.

### 2.2.1 Installation

Select one of the following ways to install F-Secure Mobile Security on your device:

- Download the installation file to your computer and move it to the device,
- Download the installation file to your computer and install the product via Nokia PC Suite, or
- Download the installation directly to your device. Installation starts automatically.

## Installation on the Device

1. Download the installation file to your computer and move it to the device or download the installation directly to your device.
2. If you downloaded the installation file directly, the installation starts automatically. Otherwise, find and open the installation file that you moved to the device.
3. When the installation is ready, restart your device if the installation asks you to do so.
4. After the installation, you need to activate the product. The product does not protect your device if you have not activated it.

## Installation Using Your Computer

To install F-Secure Mobile Security on your device using a computer, you must have the .sis installation file and Nokia PC Suite installed on your computer.

1. Connect your device to your computer.
2. Double-click the installation file to start the installation.
3. When the installation is ready, restart your device if the installation asks you to do so.
4. After the installation, you need to activate the product. The product does not protect your device if you have not activated it.

### 2.2.2 Activating the Update Service

How you activate the update service depends on where you bought F-Secure Mobile Security from. There are two main ways to activate the update service:

- by using the free-trial period, if it is available.
- by using a subscription number.

### To start the activation:

1. Open the application.
2. Select the activation type:
  - To start the evaluation period, select **Free evaluation** as the activation type if it is available and press **Done**, or
  - To have the fully licensed version, select **Subscription number** as the activation type, and press **Done**. Enter your subscription number and press **OK**.

If you do not have a subscription number, you can for example purchase a subscription number from the F-Secure estore; <http://www.f-secure.com/estore>.
3. Press **Yes** to connect to the update service and start downloading the updates.

The application connects to the update service and submits your subscription number. During the first update, the application downloads the latest virus definition database. For more information, see “*Keeping the Application Up-to-Date*”, 19.
4. When the download is complete, a message informs you that the registration was successful and that the application is activated. Press **OK** to continue.
5. After you have finished the activation, scan your device for viruses to make sure your device is clean. For instructions, see “*Manual Scanning*”, 15. The default firewall level after the installation and activation is *Normal*.



*You should scan your device whenever the application asks you to.*

## 2.3 Transferring Subscription to a New Device

You can transfer your subscription to a new device a maximum of four times. The procedure is the same as for normal installation and activation. For instructions, see “*Getting the Product Running on Your Device*”, 8.

## 2.4 Uninstalling



**IMPORTANT:** Scan your device, and remove all quarantined and infected files before you uninstall F-Secure Mobile Security.

### To uninstall the application:

1. Open the application.
2. Select **Options > Exit** to shut down the application.
3. Open **Application Manager** on your device.
4. Scroll to F-Secure Mobile Security.
5. Select **Options > Remove**.
6. Press **Yes** to confirm the uninstallation.


# 3

## USING F-SECURE MOBILE SECURITY

Opening and Closing the Application .....	13
Scanning for Viruses .....	14
Using Firewall .....	17
Keeping the Application Up-to-Date .....	19
Purchasing Subscription Service Time .....	21
Troubleshooting .....	22

## 3.1 Opening and Closing the Application

After you have activated F-Secure Mobile Security, it starts up automatically every time you turn on your device. If you have selected the manual scanning mode, you need to start the application manually:

1. Press the **Menu** key and scroll to the  icon.
2. Select **Options > Open**.



*When the real-time scanning mode is enabled, F-Secure Mobile Security runs on the background automatically. For more information, see “Real-time Scanning”, 14.*

### Closing the User Interface

Pressing the **Done** soft key hides the user interface, but keeps the application running on the background, scanning your files for viruses automatically when they are accessed (only when the real-time scanning mode is enabled). The firewall protects the system.

To shut down F-Secure Mobile Security completely, select **Options > Exit**.



**IMPORTANT:** *If you shut down the application, infected files are no longer quarantined and the system is not protected against viruses. Shutting down the application disabled the firewall.*

## 3.2 Scanning for Viruses

The application 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.

### 3.2.1 Selecting the Virus Protection Mode

1. In any of the main views, press **Options > Settings**.
2. Go to **Virus protection** and press **Options > Change** to change the virus protection mode.
  - *Real-time* - F-Secure Mobile Security runs on the background and scan files when they are accessed or modified. For more information, see “*Real-time Scanning*”, 14.
  - *Manual Scan* - F-Secure Mobile Security scans files only when you run the virus scan yourself. For more information, see “*Manual Scanning*”, 15.
3. Press **OK**.

#### Real-time Scanning

The real-time scan scans files for malicious content automatically when they are accessed or modified and when they are copied to the device.

#### Virus Alerts

When F-Secure Mobile Security detects a virus during a real-time scan, the virus is quarantined and added to the Infections list immediately.

F-Secure Mobile Security alerts you about viruses detected during the real-time scan. You can press **Yes** to view details about the infected file. For more information, see “*Processing Infected Files*”, 15.

## Manual Scanning

To scan all files on your device and the inserted memory card, follow these instructions:

1. Select **Options > Scan all**.
2. After the virus scan is finished, the application displays the following information:

Infected	The number of infections found. For more information about removing infected files, see <i>"Processing Infected Files", 15</i>
Not Scanned	The number of the files that were not scanned during the scan. A file cannot be scanned if another program has locked it or if the file is corrupted, or if you selected to skip the scan of a large file.
Scanned	The number of the files that were scanned.

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

### 3.2.2 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.

To process infected files, follow these instructions:

1. You can process infected files in the **Infections** view or **Infection details** view:
  - a. In the **Infections** view, select the infected file to be processed and press **Options > Process**.
  - b. In the **Infection details** view, press **Process**.

2. From the **Select action** menu, select the desired action, and press **OK**.

You can process the infected files in one of the following ways:

- **Quarantine** - quarantine the infected file. A quarantined file is locked and cannot harm your device when F-Secure Mobile Security is on.
- **Delete** - delete the infected file. This is the recommended option. The file will be removed completely from your device.
- **Release** - release the quarantined file. If you release a file, it will not be locked any more. You access it 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/>

## File Details

To view the list of infected files or files that were not scanned, follow these instructions:

1. In the Scan results view, select the category you want to view and press **Show**.
2. Scroll to the file that you want to view the details of which you wish to view and press **Options > Details**.

## 3.3 Using 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.

By default, the firewall protection level is set to *Normal*. This level gives you good protection and does not affect using the most common applications.

### 3.3.1 Selecting the Protection Level

The firewall has the following 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. Recommended level.	Good protection
High	Allows most commonly used applications.	High protection
Deny All	Stops all network traffic. You cannot use your e-mail, MMS or web services.	Total protection.
Custom	Allows traffic based on your custom rules.	

To change the protection level, press **Options > Change** and choose the level. To use your custom rules, select *Custom* level.

### 3.3.2 Editing Custom Firewall Rules

To edit your custom rules, select **Options > Edit FW Custom Rules**. To use your custom rule set, make sure that you have selected *Custom* as the current protection level.

## TCP/UDP

On the *TCP/UDP* view, you can add your own custom firewall rules.

To create a new rule:


1. Select **Options > Add rule**.
2. Select **Rule name** and enter a name for the new rule.
3. Select **Type** and choose the rule type.
  - Select *Normal* if you want to keep defined ports open all the time.
  - Select *Trigger* if you want to open defined ports only when some other network connection exists.
  - Select *Custom* if you want to allow other protocol than TCP or UDP traffic. Define the protocol by its number in the **Protocol number** field.
4. Select **Protocol** and choose whether you want to allow TCP or UDP Protocol traffic.
5. Select **Direction** and choose the direction of the traffic you want to allow.
6. In **Port type**, select *One port* and enter the port number you want to open in the **Port** field, or select *Port range* to define a range of ports that you want to open.
7. Select **Back** to save the rule as a new custom rule.

To remove a custom rule, select **Options > Remove rule**. Select **Options > Reset rules** to remove all custom rules.

## ICMP

On the *ICMP* view, select ICMP messages that you want to allow or deny.

- Select **Allow in** to allow all incoming and deny all outgoing messages.
- Select **Allow out** to allow all outgoing and deny all incoming messages.
- Select **Allow all** to allow both incoming and outgoing messages.
- Select **Deny all** to deny both incoming and outgoing messages.

 We recommend that you do not edit these rules unless you are familiar with the ICMP protocol. Wrong settings in these rules may cause some of your applications not to work as intended.


## Other

On the *Other* view, select whether you want to allow or deny all IPv6 and localhost traffic.

## 3.4 Keeping the Application Up-to-Date

F-Secure Mobile Security includes an automatic update service, which means that the virus definition database in the application is updated regularly. Only an up-to-date virus definition database protects your device against the latest viruses.

The application requires an active Internet connection for the updates. When a connection to the Internet is available, the application checks when the virus definition database was last updated and downloads new updates if necessary.

 *You can freely update F-Secure Mobile Security as long as you have an active subscription. To keep your device continuously protected, purchase additional service time well before the expiration date.*

### 3.4.1 Selecting the Update Mode

Automatic updates are in use after you have activated the product. If you disable automatic updates or do not use real-time scanning mode, you need to update the application manually.

To change the update mode, follow these instructions:

1. Press **Options > Settings**.
2. Go to Automatic Update and press **Options > Change**.
3. Select one of the following options:
  - **Always** (recommended) - the application downloads regular updates from the update server automatically to keep the virus definition database up-to-date.
  - **Never** - the virus definitions are not updated automatically. It is not recommended to disable automatic updates.
  - **In home network** - the application downloads updates from the update server automatically when your device is connected to the home network

### Manual Updates

To update the application manually, follow these instructions:

1. In any of the main views, press **Options > Update**.
2. Select the Internet access point to connect to the update server. The application downloads the latest virus definition database and takes it 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 "[Manual Scanning](#)", 15.

## 3.4.2 Application Updates

When a new F-Secure Mobile Security version is available, a message asks you to download it. The application restarts automatically when the update is completed.



*If the virus definition database update requires a software update to work properly, the upgrade is downloaded automatically.*

### Upgrading the Application Manually

If you want to upgrade F-Secure Mobile Security, install the new version. For instructions, see “[Getting the Product Running on Your Device](#)”, 8.

If you have F-Secure Anti-Virus installed on your device and you want to upgrade it to F-Secure Mobile Security, follow these instructions:

1. Write down your current key code. You need it to activate the new version.
2. Uninstall the installed version.
3. Download the new version.
4. Install F-Secure Mobile Security. For more information, see “[Getting the Product Running on Your Device](#)”, 8.
5. Activate the new version with your key code. For instructions, see “[Activating the Update Service](#)”, 9.

## 3.5 Purchasing Subscription Service Time

If your subscription expires, your device is no longer protected. Therefore, it is recommended that you purchase additional service time before the expiration date. The expired application displays the scanning and firewall statistics but it does not scan any files or block any network traffic.

F Secure Mobile Security warns you before the service expires.

Additional service time is added to the time remaining in your current subscription or to your free evaluation period.

F-Secure Mobile Security supports several purchase methods depending on the distribution channel. Press **Buy** to view all available purchase methods. Most common purchase methods are:

- The operator-specific continuous service subscription
- F-Secure eStore
- Your local reseller
- SMS payment

### Using PC

To purchase more service subscription time through your PC browser, follow these instructions:

1. Open <http://www.f-secure.com/estore/avmobile.shtml> in the web browser with your 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.

### Using SMS

To purchase more subscription service time by sending an SMS (only if enabled by your operator), follow these instructions:

1. Go to the *Subscription Info* screen.
2. Press **Purchase**. The *Select Method* screen is displayed.
3. Press **Options** > **Select** to select the **Phone bill** payment method.
4. When prompted to accept payment, press **OK** to complete your subscription service time purchase.
5. In the response SMS, you receive a confirmation of your purchase and a code for activating the service.

## 3.6 Troubleshooting

For troubleshooting instructions and answers to frequently asked questions, see <http://mobile.f-secure.com/FAQ/faqs60.html>.

# Technical Support

Overview.....	26
Virus Descriptions on the Web .....	26
Electronic Mail Support.....	26

## 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/>.

## 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/>.

## 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 Mobile Security 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 protects consumers and businesses against computer viruses and other threats from the Internet and mobile networks. We want to be the most reliable provider of security services in the market. One way to demonstrate this is the speed of our response. According to independent studies in 2004, 2005 and 2006 our response time to new threats is significantly faster than our major competitors. Our award-winning solutions are available for workstations, gateways, servers and mobile phones. They include antivirus and desktop firewall with intrusion prevention, antispam and antispyware solutions. Founded in 1988, F-Secure has been listed on the Helsinki Exchanges since 1999, and has been consistently growing faster than all its publicly listed competitors. F-Secure headquarters are in Helsinki, Finland, and we have regional offices around the world. F-Secure protection is also available as a service through major ISPs, such as Deutsche Telekom, France Telecom, PCCW and Charter Communications. F-Secure is the global market leader in mobile phone protection provided through mobile operators, such as T-Mobile and Swisscom and mobile handset manufacturers such as Nokia. The latest real-time virus threat scenario news are available at the F-Secure Data Security Lab weblog at <http://www.f-secure.com/weblog/>

