

F-Secure Mobile Security

for Windows Mobile

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

About This Guide	1
How This Guide Is Organized	2
Conventions Used in F-Secure Guides	3
Chapter 1 Introduction	5
1.1 F-Secure Mobile Security	6
1.2 Key features	7
Chapter 2 Installation and activation	8
2.1 System requirements	9
2.2 Getting the product running on your Windows Mobile	9
2.2.1 Installation	9
2.2.2 Activating the update service.....	11
2.3 Transferring subscription to a new device.....	12
2.4 Uninstalling F-Secure Mobile Security	12
Chapter 3 Using F-Secure Mobile Security	14
3.1 Opening and closing the application	15
3.2 Scanning for viruses.....	16
3.2.1 Selecting the virus protection mode	16
3.2.2 Processing infected files.....	18
3.3 Using firewall.....	19
3.3.1 Selecting the protection level.....	19

3.4	Protecting confidential information	20
3.4.1	Using the remote Anti-theft.....	20
3.4.2	Using the security code	21
3.4.3	Using the SMS alert.....	22
3.5	Protecting web browsing	22
3.5.1	Using Browsing Protection	22
3.6	Keeping F-Secure Mobile Security up-to-date	23
3.6.1	Selecting the update mode.....	24
3.7	Purchasing subscription service time	26
3.8	Troubleshooting	27

Chapter 4 Technical support 28

Overview	29
----------------	----

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 and activation.* Gives instructions on installing and setting up F-Secure Mobile Security.

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

Chapter 4. *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.

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.

1

INTRODUCTION

F-Secure Mobile Security	6
Key features	7

1.1 F-Secure Mobile Security

F-Secure Mobile Security is a software product that protects data stored on your Windows Mobile device against malicious code attacks and in case your device is lost or stolen. It also protects the device from network intrusion attempts and protects you from web sites that may steal your personal information.

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 scans all files when they are accessed. You can also manually scan your device for viruses whenever you want.
Automatic updates	The application downloads regular updates to keep the virus definition database up-to-date automatically.
Firewall	The application protects you from potential network harm by blocking connections that do not meet the set security criteria.
Anti-theft	You can remotely lock your mobile device or wipe the data stored on the device if it is stolen.
Browsing protection	The application protects you from web sites that may steal your personal information, including credit card numbers, user account information, and passwords.

2

INSTALLATION AND ACTIVATION

System requirements.....	9
Getting the product running on your Windows Mobile.....	9
Uninstalling F-Secure Mobile Security.....	12

2.1 System requirements

You can find a list of supported devices at the internet address:
<http://mobile.f-secure.com/devices/>

2.2 Getting the product running on your Windows Mobile

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

1. First, you must install F-Secure Mobile Security, see “*Installation*”, 9.
2. Then you must activate your antivirus subscription, see “*Activating the update service*”, 11.

2.2.1 Installation

There are two ways to install F-Secure Mobile Security on your Windows Mobile device, depending on the type of installation file you have:

- Directly on your mobile device (.cab file),
- By using ActiveSync and your computer (.exe file).

Direct installation

1. Transfer the .cab installation file to your Windows Mobile device or download the file with the mobile device browser at <http://mobile.f-secure.com/downloads.html>.
2. Locate this .cab file in File Explorer on your Windows Mobile device.
3. Tap the .cab file to start the installation process.
4. After installing the application, you may need to restart your Windows Mobile device. Tap **Yes** to do so.

5. After the installation, you need to activate the product. The product does not protect your device if you have not activated it. See [“Activating the update service”](#), 11.

Installation using your computer

To install F-Secure Mobile Security on your Windows Mobile device using a computer, you must have the .exe installation file and Microsoft ActiveSync version 3.7.1 or later on your computer.

To install F-Secure Mobile Security using a computer:

1. Run the installation program by double clicking the F-Secure Mobile Security .exe file on your computer.
 - If your Windows Mobile device is connected to your computer, ActiveSync will install F-Secure Mobile Security immediately.
 - If your Windows Mobile device is not connected to the computer during the installation process, ActiveSync installs F-Secure Mobile Security during the next ActiveSync session.
2. After installing the application, you may need to restart your Windows Mobile device. Tap **Yes** to do so.
3. After the installation, you need to activate the product. The product does not protect your device if you have not activated it. See [“Activating the update service”](#), 11.

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 code.

Activating the free-trial period

If the free-trial is available, you can activate your free-trial period when you launch the application for the first time.

To activate the free-trial:

1. Tap **Yes** on the activation dialog that appears when you switch your Windows Mobile device on for the first time after installing F-Secure Mobile Security.
2. Tap **Free Evaluation**.
3. Tap **Next**.
4. Tap **Yes** to confirm the connection to the update server.
5. After the update has finished, select **Ok**.

Using a subscription code

If the free-trial period is unavailable, you have to use a subscription code to activate the application.

If you do not have a subscription number, you can purchase a subscription number from the F-Secure estore:

<http://www.f-secure.com/estore>.

To activate the update service with a subscription code:

1. Tap **Yes** on the activation dialog that appears when you switch your Windows Mobile device on for the first time after installing F-Secure Mobile Security.
2. Tap **Subscription Number**.

3. Tap **Next**.
4. Enter your subscription number.
5. Tap **Next**.
6. Tap **Yes** to confirm the connection to the update server.
7. Select **Ok**.

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 Windows Mobile](#)”, 9.

2.4 Uninstalling F-Secure Mobile Security

You can uninstall F-Secure Mobile Security in two ways:

- On your Windows Mobile device,
- By using ActiveSync and your computer.



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

Direct uninstallation

To uninstall F-Secure Mobile Security from your Windows Mobile device, follow these instructions:

1. Close the application by selecting **Exit** from the menu on the main view.
2. Tap **Yes** to confirm that you want to disable F-Secure Mobile Security.
3. On the **Start** menu, tap **Settings**, select **System** and then tap **Remove programs**.
4. Select **F-Secure Mobile Security** and tap **Remove**.

5. Tap **Yes** when you are prompted if you want to uninstall the application.

Uninstallation with your computer

To uninstall F-Secure Mobile Security using your computer, follow these instructions:

1. Close the application by selecting **Exit** from the menu on the main view.
2. Connect your Windows Mobile device to your computer.
3. Start ActiveSync on your computer.
4. Click **Add/Remove Programs** on the ActiveSync **Tools** menu.
5. From the list of installed applications, select **F-Secure Mobile Security**, and click **Remove**.

3

USING F-SECURE MOBILE SECURITY

Opening and closing the application.....	15
Scanning for viruses.....	16
Using firewall.....	19
Protecting confidential information.....	20
Protecting web browsing.....	22
Keeping F-Secure Mobile Security up-to-date.....	23
Purchasing subscription service time.....	26
Troubleshooting.....	27

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.

To open the user interface:

1. Select **Start** →  **Mobile Security**.
2. If you are prompted to run a virus scan, tap **Yes**.



When the real-time scanning mode is turned on, F-Secure Mobile Security runs on the background automatically. For more information, see “Real-time scanning”, 16.

Closing the user interface

Press the close icon to hide the user interface. When the user interface is hidden, the application keeps running on the background, scanning your files for viruses automatically when they are accessed if the real-time scanning mode is enabled, and the firewall protects the system.

To shut down F-Secure Mobile Security completely, select **Exit** from the menu on the main view.



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 disables the firewall, Anti-Theft, and Browsing Protection features.*

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. Tap **Settings** in the main view.
2. Tap **Virus protection** in the settings selection list.
3. Select either the real-time or the manual **Virus protection** mode.
 - Check the *Real-time protection* check box to keep F-Secure Mobile Security running on the background and scanning files when they are accessed or modified. All infected files are quarantined automatically. For more information, see “*Real-time scanning*”, 16.
 - Leave the check box unchecked to disable the real-time scan. Files are not scanned automatically. You should manually scan your device each time you transfer any new data to it. For more information, see “*Manual scanning*”, 17.
4. Tap **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. Tap the infected file to view details about the infection. For more information, see “*Processing infected files*”, 18.

Manual scanning

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

1. Tap **Virus protection** in the main view.
2. Tap **Scan now**.
3. 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", 18</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.
Scanned	The number of the files that were scanned.

4. Tap **ok** 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. Tap **Virus protection** in the main view.
2. Tap **Infected files**.
3. In the *Infections* view, tap the infected file you want to process.
4. Choose one of the following actions:
 - **Delete** - delete the infected file. This is the recommended option. The file will be removed completely from your device.
 - **Quarantine** - quarantine the infected file. A quarantined file is locked and cannot harm your device when F-Secure Mobile Security is on.
 - **Release** - release the quarantined file. If you release a file, it will not be locked any more. You access it at your own risk.



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

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

To select the security level:

1. Tap **Settings** in the main view.
2. Tap **Firewall** in the settings selection list.
3. Select the firewall level you want to use.

The firewall has the following protection levels:

Level	Description	Protection
Deny All	Stops all network traffic. You cannot use your e-mail, MMS or web services.	Total protection
High	Allows most commonly used applications.	High protection
Normal	Allows all outgoing connections. Recommended level.	Good protection
Allow All	Allows all network traffic. Does not stop any incoming or outgoing connections.	No protection
Custom	Allows network traffic based on your custom rules.	Tap Edit custom ruleset to edit the custom rules.

3.4 Protecting confidential information

With Anti-theft, you can make sure that your device or data stored on it is not misused if your device is stolen and Anti-theft can alert you if somebody changes the SIM card in your device.

3.4.1 Using the remote Anti-theft

With the remote lock, you can lock the device remotely by sending it an SMS message you have created. The locked device can be unlocked only with the lock code of your device. To use the remote lock, keep the device lock turned on.

With the remote wipe, you can wipe the device remotely by sending it an SMS message you have created. When the device is wiped, the application deletes all the information stored in the device memory.

 *As memory cards can be easily removed, store your confidential information in the device memory.*

To set up remote lock and wipe:

1. Tap **Settings** in the main view.
2. Tap **Anti-theft** in the settings selection list.
3. Select which features you want to turn on:
 - If you want to be able to wipe your device remotely, select **Enable remote wipe**.
 - If you want to be able to lock your device remotely, Select **Enable remote lock**.

 *You can enable the remote lock only when the device lock is turned on.*

4. Enter your **Security code** and type it again to confirm it.

To lock or wipe your device remotely:

- To lock the device, send the following SMS message to your device:
#LOCK#<security code> (For example: #LOCK#abcd1234)
Locked device can be unlocked only with the system lock password.
- To wipe the device, send the following SMS message to your device:
#WIPE#<security code> (For example: #WIPE#abcd1234)
When the device is wiped, all data stored on it is removed.

3.4.2 Using the security code

You can use the security code to remotely lock or wipe your device.

The security code needs to be at least 8 characters long. Use a code that is easy to remember but hard to guess. Store the security code in a safe place.

To set up the security code:

1. Tap **Settings** in the main view.
2. Tap **Anti-theft** in the settings selection list.
3. Enter your **Security code** and type it again to confirm it.



At least one of the remote anti-theft features has to be turned on before you can enter the security code.

Unlocking the Locked Device

To unlock the locked device, enter the lock code of your device.

3.4.3 Using the SMS alert

You can set Anti-theft to send you an SMS text message when somebody changes the SIM card in your device.

To use the SMS alert, turn on the **SMS alert when SIM changed** setting and specify the phone number where the SMS text message should be sent when the SIM card in the device is changed.



You can send the lock or wipe message to the number from where you received the SMS alert to remotely lock or wipe your device.

3.5 Protecting web browsing

Browsing Protection protects you from web sites that may steal your personal information, including credit card numbers, user account information, and passwords.

Browsing Protection checks web sites that you browse with Internet Explorer. Browsing Protection is turned on automatically after you have activated F-Secure Mobile Security if Internet Explorer is set as your default browser. If you use any third-party browser, Browsing Protection does not protect your web browsing.

3.5.1 Using Browsing Protection

To turn on Browsing Protection:

1. In the main view, open **Browsing Protection**.
1. In the Browsing Protection menu, select **Settings**.
2. If you want to turn on Browsing Protection, select **Enable Browsing Protection**.

3. In **Network to use**, select whether you want to use Browsing Protection all the time or only when you are browsing the web on your own operator's network:
 - Select **My operator only** to use Browsing Protection only when you are using your own operator's network.
 - Select the **All operators** setting to keep the protection turned on when you are travelling and outside of your own operator's network.

When you try to enter to a web site that contains harmful content, Browsing protection notifies you and blocks the access to the harmful site. Select **Go back** to return to the page where you left.

If you want to enter the site even though Browsing protection blocked it, follow the [I want to enter this web site anyway](#) link in the block page.

3.6 Keeping F-Secure Mobile Security 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.

3.6.1 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. Tap **Settings** in the main view.
2. Tap **Virus protection** in the settings selection list.
3. Select one of the following *Automatic updates* mode.
 - *Always* - the application downloads regular updates from the update server automatically to keep the virus definition database up-to-date.
 - *In home network* – the application downloads updates from the update server automatically when your device is connected to the network of your service provider. (recommended)
 - *Never* – the virus definitions are not updated automatically. We do not recommend that you disable automatic updates.

Manual updates

1. Tap **Virus protection** in the main view.
2. Tap **Update now**.
3. The application requires a network connection. Tap **Yes** when the connection the update server is needed.
4. The application downloads the latest virus definition database and takes it into use immediately.
5. When the update is complete, tap **Yes** to scan your device for viruses. For more information on scanning, see "*Manual scanning*", 17.

Application Updates

If a new version of the application is available when you tap **Update now**, the application notifies you and you can download it. The application restarts automatically when the update is completed.

 *If the automatic update is turned on, critical application updates are installed 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 Windows Mobile](#)”, 9.

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.
To find your key code, select **Menu→About** in the main view.
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 Windows Mobile](#)”, 9.
5. Activate the new version with your key code. For instructions, see “[Activating the update service](#)”, 11.

3.7 Purchasing subscription service time

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

F-Secure Mobile Security supports several purchase methods depending on the distribution channel. Most common purchase methods are:

The operator-specific continuous service subscription

- F-Secure eStore
- Your local reseller
- Openbit SMS payment

If you wish to purchase F-Secure Mobile Security after using the trial version, use the subscription code provided in the *About* view. If you received a new subscription code when you purchased service time or a new license, use it to activate the software. For more information, follow the instructions in the purchase menu.

Using your Windows Mobile

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

1. Tap **Buy** in the main view.
2. Select the payment method you want to use.
3. Follow the instructions on the screen.

Using PC

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

1. Open <http://www.f-secure.com/estore/> in the web browser with your computer.
2. Enter your subscription code in the *Subscription Code* 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.

3.8 Troubleshooting

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

4

TECHNICAL SUPPORT

Overview.....	29
Virus descriptions on the web.....	29
E-mail support	29

Overview

F-Secure Technical Support is available by e-mail and from our Web site. You can access our Web site from within the product 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/en_EMEA/security/.

E-mail support

If you have questions about the product 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

Example: Anti-Virus-Norway@F-Secure.com

If there is no authorized F-Secure Business Partner in your country, you can request basic technical assistance from: 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 online threats from the Internet and mobile networks. We want to be the most reliable provider of internet security services in the market. One way to demonstrate this is the speed of our response.

F-Secure's award-winning solutions for real-time virus protection are available as a service subscription through more than 170 Internet service providers and mobile operator partners around the world, making F-Secure the global leader in the market of internet and computer security. The solutions are also available as licensed products through thousands of resellers globally.

F-Secure aspires to be the most reliable mobile and computer security provider, helping make computer and smartphone users' networked lives safe and easy. This is substantiated by the company's independently proven ability to respond faster to new threats than its main competitors. Founded in 1988 and headquartered in Finland, F-Secure has been listed on the OMX Nordic Exchange Helsinki since 1999. The company has consistently been one of the fastest growing publicly listed companies in the industry.

The latest news on real-time virus threat scenarios is available at the <http://www.f-secure.com/weblog/>

