

F-Secure Mobile Security™ for S60

1. Installing and activating

Previous version You do not need to uninstall the previous version of F-Secure Mobile Anti-Virus. Check the F-Secure Mobile Security settings after you have installed the new version.

Installing **To install:**

- 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.

After the installation, restart the device if the installation asks you to do so. When the installation is ready, you need to activate the product. The product does not protect your device if you have not activated it.

Activating **To start the activation:**

1. Open the application. The Welcome screen is displayed.
2. Press **Continue**.
3. Select the activation type:
 - To activate the product with only the Anti-theft feature active, select **Anti-theft only** as the activation type and press **Continue**.
 - To have the fully licensed version, select **Subscription number** as the activation type, and press **Continue**. Enter your subscription number and press **OK**.
4. Press **Yes** and select the Internet access point 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.
5. After the product has downloaded all the necessary updates, the application is complete. Press **Continue** to finish the activation.

After you have finished the activation, scan your device for viruses to make sure your device is clean. See the [Scanning for viruses](#) section below.



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

2. Scanning for viruses

F-Secure Mobile Security works in the background and scans your files automatically.

1. F-Secure Mobile Security notifies you if it finds a virus during the real-time scan. Press **Yes** to view infected files immediately or **No** to view them later.
2. The infections view contains a list of infected files on the device and whether the file is currently quarantined or released.

To view more details about an infected file:

1. Scroll to the infected file and press the selection key.
2. Select **View**.
3. 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.

Processing infected files

To process infected files:

1. In the infections view, scroll to the infected file you want to process.
2. Press the selection key.
3. 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 if it is not quarantined already. 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.

3. Preventing unauthorized network traffic

The firewall in F-Secure Mobile Security works quietly in the background. It monitors incoming and outgoing Internet and network traffic, and protects you from intrusion attempts. The predefined firewall levels allow you to change the level of protection according to your needs.


Selecting security level

To select the security level:

1. Browse to **Settings** and press the selection key.
2. Select **Firewall** from the settings selection list.
3. Select the desired firewall level:
 - **Deny All** - stops all network traffic.
 - **High** - allows most commonly used applications and blocks all incoming traffic.
 - **Normal** - allows all outgoing connections and blocks all incoming traffic.
 - **Allow All** - allows all network traffic.
 - **Custom** - allows network traffic based on your custom rules. To edit the custom rule set, select **Options > Edit custom rules** when the **Custom** security level is selected.

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.


 *As memory cards can be easily removed, store your confidential information in the device memory that you can lock and wipe with Anti-theft.*

Using the device lock

Anti-theft can automatically lock your device when the SIM card in the device is changed. The locked device can be unlocked only with your lock code.

To set up the device lock:

1. Browse to **Settings** and press the selection key.
2. Select **Anti-theft** in the settings selection list.
3. Enter a **Lock code**. The lock code needs to be at least 5 characters long. Store it in a safe place.

 *Your lock code protects the Anti-theft settings. You have to enter your current lock code before you can change any Anti-theft settings.*

4. If you want to lock your device when a SIM card changes, select **Yes** on **Lock when SIM changed**.

Using the remote anti-theft

With remote anti-theft, you can send an SMS text message that contains your lock code to your device to locate it or lock it or wipe code to wipe all information in it.

To set up remote lock:

1. Browse to **Settings** and press the selection key.
2. Select **Anti-theft** in the settings selection list.
3. If you want to be able to lock your device remotely, follow these instructions:
 - a. Enter a **Lock code** if you have not created it yet.
 - b. Turn on **Remote lock**.The locked device can be unlocked only with your lock code.
4. If you want to be able to wipe your device remotely, follow these instructions:
 - a. Enter a **Wipe code**. The wipe code needs to be at least 8 characters long. Store it in a safe place.
 - b. Turn on **Remote wipe**.

When the device is wiped, all data stored on it is removed.

To lock or wipe your device remotely:


Send the following SMS text message to your device.

- To lock the device, send:
#LOCK#<lock code> (For example: #LOCK#abcd1234)
- To wipe the device, send:
#WIPE#<wipe code> (For example: #WIPE#abcd1234)
- To locate the device, send:
#LOCATE#<lock code> (For example: #LOCATE#abcd1234)

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 the default browser of your device. If you use any third-party browser, Browsing protection does not protect your web browsing.

 *Turn off the web browser and clear its cache before you start using the browsing protection.*

To turn on Browsing protection:


1. Browse to **Settings** and press the selection key.
2. Select **Browsing protection** in the settings selection list.
3. Turn on **Browsing protection**.
4. 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.

Privacy mode

Browsing protection can send information of web sites that contain harmful content to the analysis automatically to maintain the quality of service. You can choose which information you want to submit to the analysis.

To change the privacy mode:

1. Browse to **Settings** and press the selection key.
2. Select **Other settings** in the settings selection list.
3. In Privacy mode, select
 - Select **Statistics only** to submit only browsing protection statistics and the server connection information.
 - Select **Allow all** to submit statistics and information on web sites that have not been analysed or contained harmful content.

 *For the best quality of service, we recommend that you keep the privacy mode as **Allow all**.*

Privacy statement

Submitting information does not compromise your privacy.

Even though the submitted information may be considered personal under some jurisdictions, your privacy is protected during the process. We transfer the information securely, remove any unnecessary personal information, and process the information anonymously in an aggregate format. In this way, the information cannot be connected to you in any way. No user account information, no IP address information, or no license information is included in the information you submit. We protect your privacy further by using encryption when transferring the information.

The submitted information is used for improving the protection capabilities of our services and products.

6. Keeping the product up-to-date

Automatic updates

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. Automatic updates are in use after you have activated the product.

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.

Manual updates

To update the application manually:

1. Browse to **Virus protection** and press the selection key.
2. Select **Update now**.
3. 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.
4. When the update is finished, press **Yes** to scan your device for viruses if you are prompted to do so. See the **Scanning for viruses** section above.

Version 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.

Technical support

The main view of the user interface displays the security overview and the current status.

If the status displays that your device is not protected, follow these instructions:

1. Browse to **Security overview** and press the selection key.
2. Select the item with either red or yellow status icon and press the selection key to solve the issue.

For more information, download the *F-Secure Mobile Security for S60 User's Guide* (available in English) at <http://mobile.f-secure.com/>

If you have questions about the application not covered in the guides or in the online services, you can contact your local F-Secure distributor or F-Secure Corporation directly.

DISCLAIMER

"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 © 2009 F-Secure Corporation. All rights reserved

