

F-Secure Mobile Security with Parental control

S60

Contents

Chapter 1: Overview.....	5
Key features.....	6
Chapter 2: Installation.....	7
System requirements.....	8
Install and activate the product.....	8
Installation on the device.....	8
Installation using your computer.....	8
Activating.....	9
Transferring the subscription to a new device.....	9
Uninstalling.....	9
Opening and closing the product.....	10
Opening the application.....	10
Closing the user interface.....	10
Chapter 3: Using the product.....	11
Scanning for viruses.....	12
Selecting the virus protection mode.....	12
Processing infected files.....	13
Using Firewall.....	13
Selecting the protection level.....	13
Protecting confidential information.....	14
Using the device lock.....	14
Turning on remote Anti-Theft.....	15
Using the SMS alert.....	16
Using Anti-Theft alarm.....	16
Retrieving a forgotten security code.....	16
Protecting web browsing.....	17
Using Browsing protection.....	17
Using the Internet safely.....	17
Privacy mode.....	18
Making browsing safe for children.....	18
What are age groups.....	19
Selecting user's age group.....	20
Keeping the application up-to-date.....	20
Selecting the update mode.....	21
Manual updates.....	21
Application updates.....	21

Purchasing subscription service time.....22
 Purchasing subscription service time with SMS.....22
 Purchasing subscription service time with credit card.....22
 Purchasing subscription service time with your PC.....22

Chapter 4: Technical support.....23
 Security overview.....24

Overview

Topics:

- [Key features](#)

F-Secure Mobile Security provides complete security for your mobile device.

The product protects data stored in your mobile device against malicious code attacks and monitors incoming and outgoing connections and protects the device from network intrusion attempts. It also helps you protect your personal and confidential data in the event your device is lost or stolen. Browsing protection identifies which web sites are safe and which web sites you should avoid, and automatically blocks harmful sites to ensure you are safe on the Internet.

The product 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 in the background.

To work effectively, antivirus software requires an always up-to-date virus definition database. The product retrieves the latest virus definition databases automatically.

Key features

The list of key features in the product.

The product 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.
Anti-theft	The application protects your confidential information by locking the device automatically when the SIM card is changed. You can also send a message to your mobile device to locate it or remotely wipe the data stored on it 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.

Installation

Topics:

- [System requirements](#)
- [Install and activate the product](#)
- [Transferring the subscription to a new device](#)
- [Uninstalling](#)
- [Opening and closing the product](#)

Instructions how to install the product on the mobile device.

Select one of the following ways to install the product on your device:

- Install the application directly on the device, or
- Download the installation file to your computer and install the product via Nokia PC Suite.

After you have installed the product, you need to activate it. Activating the product turns on the protection.

System requirements

The list of minimum system requirements to install and use the product.

To use the product, your device must meet the following requirements:

Platform:	Nokia S60 (3rd or 5th 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.

Install and activate the product

Instructions how to install and activate the product.

Installation on the device

Instructions how to install the product directly on the device

You need to have the installation file on your device to start the installation. Either download the installation file to your computer and move it to the device, or download the installation directly to your device.

Follow these instructions to install the product using your mobile device.

1. If you downloaded the installation file directly, the installation starts automatically. Otherwise, find and open the installation file that you moved to the device.
2. Follow the on-screen instructions to install the product.
3. When the installation is ready, restart your device if the installation asks you to do so.

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

Instructions how to install the product with 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.

Follow these instructions to install the product using 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.


After the installation, you need to activate the product. The product does not protect your device if you have not activated it.

Activating

Activating the product turns on the protection.

Follow these instructions to activate the product:

1. Start the application.
The product displays the license terms the first time you start it.
2. Read the license terms and press **Continue** after you accept them.
The activation starts after you have accepted the license terms.
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**.
 - If you already have a subscription code, select **Subscription code** as the activation type and press **Continue**. Then enter your subscription code and press **OK**.

 **Note:** You can purchase a subscription code from the F-Secure estore:
<http://www.f-secure.com/estore>.
4. The activation requires a connection to the update service. Press **Yes** to connect to the update service.
The application connects to the update service and activates the product.
If you used the subscription code to activate the product, the application downloads the latest virus definition database during the first update.
5. After the product has downloaded all the necessary updates, the activation is complete. Press **Continue** to finish the activation.

After you have activated the product, the main user interface of the product opens and the product protects your device.

Scan your device for viruses to make sure your device is clean after you have installed and activated the product.

The default firewall level is set to normal.

Transferring the subscription to a new device

You can transfer your product subscription to your new device.

You can transfer your subscription to a new device a maximum of four times. To transfer your subscription:

Follow the normal installation and activation instructions.

Uninstalling

Instructions how to remove the product from your device.

Scan your device and remove all quarantined and infected files before you uninstall the product.

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.

The product is removed from your device.

Opening and closing the product


Instructions how to start and shut down the product.

Opening the application

After you have activated the product, 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 product icon.
2. Select **Options** > **Open**.

 **Note:** When the real-time scanning mode is turned on, the product runs on the background automatically.

Closing the user interface

When the user interface is hidden, the product still scans your files for viruses and the firewall protects the system.

To hide the user interface:

Press the **Done** soft key.


The product keeps running on the background scanning your files for viruses automatically when they are accessed (if the real-time scanning mode is turned on) and the firewall protects the system.

Shutting down the application

When you shut down the product, all the features are turned off.

To shut down the application 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 turns off the firewall, Anti-Theft, and Browsing Protection features.

Using the product

Topics:

- [*Scanning for viruses*](#)
- [*Using Firewall*](#)
- [*Protecting confidential information*](#)
- [*Protecting web browsing*](#)
- [*Making browsing safe for children*](#)
- [*Keeping the application up-to-date*](#)
- [*Purchasing subscription service time*](#)

Instructions how to use the product.

Follow the instructions in this chapter to set up and use the product to protect your data stored on your device.

Scanning for viruses

The product scans your device for viruses and other malicious code.

The product scans all files for viruses automatically when they are saved, copied, downloaded, synchronized or modified otherwise.

Selecting the virus protection mode

If you do not want to use the real-time scanning, you can manually scan all the data for viruses whenever you want.

The application scans all accessed and modified data on your device automatically for malicious content when the real-time scanning is turned on.

To change the virus protection mode:

1. Browse to **Settings** and press the selection key.
The settings selection list opens.
2. Select **Virus protection** from the settings selection list.
3. Select either the real-time or the manual virus protection mode.
 - Select **Real-time** to run the application on the background and scan files when they are accessed or modified.
 - Select **Manual Scan** to scan files only when you run the virus scan yourself.
4. 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.

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.

Manual scanning

You can scan your device for viruses and other malicious code any time you want.

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

1. Browse to **Virus protection** and press the selection key.
2. Select **Scan now**.
The virus scan starts.
3. After the scan is finished, the application displays the following information.
 - **Infected** - The number of infections found.
 - **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. Press **Back** to exit the scan.

All infected files are quarantined and cannot be accessed when the product is running in the background.

Processing infected files

When the product finds a virus or other malicious code in a file, you can remove the infected file from your device.

To process infected files, follow these instructions:

1. Browse to **Virus protection** and press the selection key.
2. Select **Infected files**.
The **Infections view** opens.
3. In the **Infections view**, scroll to the infected file you want to process.
4. Select one of the following actions:
 - **Quarantine** - quarantine the infected file. A quarantined file is locked and cannot harm your device when the product 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 the selection key, select the action you want to perform to the infected file, and press **OK**.

5. To view more details about the selected file, select **Details**. The **Infection details view** displays the path and file name of the infected file, and the name of the infection.

You can find descriptions and information on viruses, trojans, worms, and other forms of unwanted software in the F-Secure web site: <http://www.f-secure.com/virus-info/>.

Using Firewall

The firewall 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.

Selecting the protection level

Change the protection level to select the network traffic you want to allow and deny.

To select the protection level:

1. Browse to **Settings** and press the selection key.
The settings selection list opens.
2. Select **Firewall** from the settings selection list.
3. Select the firewall protection level that you want to use.

Firewall protection levels

The firewall has multiple protection levels.

Level	Description	Protection
Allow All	Allows all network traffic. Does not stop any incoming or outgoing connections.	No protection

Level	Description	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 network traffic based on your custom rules.	Customized rule set

 **Note:** To edit the custom rule set, select **Options** > **Edit custom rules** when the **Custom** protection level is selected.

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.

Anti-Theft can alert you if somebody changes the SIM card in your device.

If you lose your device, you can send an SMS text message to your device to locate it or lock it remotely.

- After the device is locked, it can be unlocked only with the security code.

 **Note:** To use the remote lock, keep the device lock turned on.

You can wipe the data in the device remotely with the remote wipe.

- When you send an SMS message to wipe your device, the product deletes all the information stored in the device memory.

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

Using the device lock

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

To set up the device lock:

1. Browse to **Settings** and press the selection key.

The settings selection list opens.

2. Select **Anti-theft** in the settings selection list.

3. Enter a **Security code**. The security code needs to be at least 4 characters long. Store it in a safe place. Your security code protects the Anti-theft settings. You have to enter your lock code before you can change any Anti-theft settings.

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

When someone inserts a new SIM card into the device and the SIM change lock is turned on, the device asks for the lock code before it can be used.

Turning on remote Anti-Theft

When remote Anti-Theft features are turned on, you can send SMS text message to your device to lock it or to wipe information in it.

To set up remote Anti-Theft:

1. In the main view, open **Anti-theft**.
2. In the **Anti-theft** menu, select **Settings**.
3. If you want to be able to lock your device remotely, follow these instructions:
 - a) Enter a **Security code** if you have not created it yet.
 - b) Turn on **Remote lock**.
4. If you want to be able to wipe your device remotely, turn on **Remote wipe**.
5. If you want to be able to locate your device remotely, turn on **Remote locate**.

To use the remote locate, make sure that the positioning methods in your device are turned on. Usually these are turned on by default. For more information, consult the documentation that came with your device.

The remote Anti-Theft is turned on.

Locking your device remotely

When you lock your device remotely, it cannot be used without your permission.

Follow these instructions to lock your lost or stolen device:

To lock the device, send the following SMS message to your device: #LOCK#<security code>
(For example: #LOCK#12345678)

Locked device can be unlocked only with the system lock password.

Wiping your device remotely

When you wipe your device, Anti-Theft deletes your personal information stored in the device.


Follow these instructions to wipe your lost or stolen device:


To wipe the device, send the following SMS message to your device: #WIPE#<security code>
(For example: #WIPE#12345678)

When you wipe the device, the product removes all data stored on it.

Locating your device

You can send an SMS message to your lost device to locate it.



 **Note:** To make sure that Anti-theft can receive the location information from the device, make sure that the **Positioning server use** setting in your device settings is set to **Automatic** and you you have configured a valid access point. To access these settings in your device, go to **Settings > General > Positioning**. For more information, consult the documentation that came with your device.

 **Note:** Make sure that **Bluetooth GPS** is turned off and all other positioning methods are turned on, otherwise your device tries to connect to an external GPS receiver when you try to locate it.

Follow these instructions to locate your device:

To locate the device, send the following SMS message to your device: #LOCATE#<security code>
(For example: #LOCATE#12345678)

Anti-Theft replies with an SMS message that contains the latest location of the device.

-  **Tip:** Send the locate message to your device after you have set it up to make sure that it works correctly.
-  **Note:** Anti-Theft does not store any location data, the only location information is in the SMS text message that is sent to you.

Using the SMS alert

You can set Anti-Theft to alert you with an SMS message when somebody changes the SIM card in your device.

To use the SMS alert:

1. In the main view, open **Anti-theft**.
2. In the **Anti-theft** menu, select **Settings**.
3. Select **Trusted number**.
The number dialog opens.
4. Specify the phone number where the SMS text message should be sent when the SIM card in the device is changed.
5. Turn on the **Report SIM change** setting.


When the SMS alert is turned on, you receive an SMS text message when the SIM card in your device is changed.

Using Anti-Theft alarm

You can play alarm sound on your device if it is lost or stolen.

Follow these instructions to play an alarm sound on your device:

1. To play an alarm, send the following SMS message to your device: #ALARM#<security code>#<repeat count>

 **Note:** You can specify how many times to play the alarm with the repeat count, but it is not necessary to play the alarm.

(For example: #ALARM#abcd1234)

2. When the device receives the message, the product locks the device and plays the alarm sound. The product sends a reply message to the phone that you used to send the alarm message.

To turn off the alarm, send the following SMS message to your device: #ALARM#<security code>#0

Retrieving a forgotten security code

You can reset a forgotten security code from the trusted number.

You need to enter the **Trusted number** phone number in Anti-theft settings to reset your security code.

If you forget your security code, you can reset it from the trusted number. Follow these instructions:

1. Send SMS with the following message to your device: #UNLOCK#
Your device sends the reset SMS message with instructions to the trusted number.
2. Send the reset code from the trusted number to your device.

Your device is unlocked and you can create a new security code.

Protecting web browsing

This chapter explains how Browsing Protection works and how you can set it up.

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.

Using Browsing protection

You need to use F-Secure Browser. If you use any other browser, Browsing Protection does not protect your web browsing.

To use the Browsing Protection while browsing the web, follow these instructions:

To start the web browser:

- Open the safe browser in the product. In the main view, select **Browsing Protection** and select **Safe browser**.
- Open **F-Secure Browser** in the Android Launcher.

Changing the default browser

Instructions how to change the default browser in your device.

F-Secure Browser is not set as your default browser automatically. If you have set a default browser already, follow these instructions to make F-Secure Browser your default browser:

1. Open **Settings > Applications > Manage Applications**.
2. Select **Browser**.
3. In **Launch by default**, select **Clear defaults**.
4. Select **F-Secure Browser** as your default web browser the next time you use some application to go to the web.

Using the Internet safely

Browsing Protection helps you evaluate the safety of web sites you visit and prevents you from accessing harmful web sites unintentionally.

The product checks the safety of a web site over the air automatically when you access the site. If the site is rated as suspicious or harmful, the product blocks the access to the site. The safety rating of a web site is based on information from several sources, such as F-Secure malware analysts and F-Secure partners.

Changing the Browsing protection settings

You can select when the Browsing Protection is turned on based on the operator network that you are using.

To change the product settings:

1. Browse to **Settings** and press the selection key.
The settings selection list opens.
2. Select **Browsing protection** in the settings selection list.

3. Turn on **Browsing protection** to keep the product running on the background while you browse the Internet.
4. Select when the Browsing Protection is in use:
 - **All operators** - the product checks the safety of visited web sites regardless of the operator network that you use.
 - **My operator only** - the product checks the safety of visited web sites only when you are using your own operator network.

When the Browsing Protection is turned on, the product blocks the access to harmful web sites. Select **Go back** in the block page 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.

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.

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.

Changing the privacy mode

You can change the privacy mode to select the type of information you want to submit.

To change the privacy mode:

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


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

Making browsing safe for children

Parental control helps you keep your children safe from the inappropriate content in the Internet.

The Internet is full of interesting web sites, but there are also many risks for children who use the Internet. Small children and teenagers are at risk as they browse the web with their mobile devices, usually unsupervised. Many web sites contain material that you might consider inappropriate for your children. They can get exposed to inappropriate material, they may accidentally download malware that could damage the mobile device, or they may receive harassing messages after browsing in unsafe web sites.

With Parental control, you can let your children browse the web safely with their mobile devices by blocking their access to unwanted content.

 **Note:** Parental control works with the default web browser and prevents your children from using other browsers.

What are age groups

With age groups, you can define web site categories that are suitable for teenagers and small children.

Parental control analyzes web pages and blocks access to unwanted web pages based on their content.

Parental control has three pre-set profiles that limit the web content in different ways. Teenagers can have more freedom to browse the Internet while small children have tighter restrictions on their online activities. The adult age group can browse the Internet without limitations.

You can select the user's age group during the installation, or later on the Parental control settings page.

Content types

By using Parental control, you can block access to several content types.

- **Adult**
Content that is clearly sexual, or contains a sexual innuendo. For example, sex shop sites or sexually-oriented nudity.
- **Chat**
For example, web-based chat programs and instant messaging programs, and chat sites.
- **Webmail**
For example, sites on which you can create e-mail accounts to send and receive messages through a web browser.
- **Weapons**
For example, sites that contain descriptions or images of weapons, or instructions for creating weapons or explosives.
- **Gambling**
For example, online gambling or lottery web sites.
- **Drugs**
Sites that promote drug use. For example, sites that contain information about growing, buying, or selling drugs.
- **Dating**
For example, matchmaking sites or mail-order bride sites.
- **Social networking**
For example, sites where you can create a member profile to share your personal and professional interests.
- **Forum**
For example, discussion groups, where you can view and post comments, or programs which you can use for creating forums.
- **Blogs**
For example, online diaries, personal web pages, blogs and podcasts.
- **Shopping and auctions**
For example, sites that allow visitors to order items directly over the web, price comparison web sites, or online auction sites.

- Cult

For example, sites that attract fanatical groups of devotees or promote attacks on religion and other ideologies.

- Alcohol and tobacco

For example, sites that provide information, promote, or support the sale of alcoholic beverages or tobacco products.

- Hate and violence

For example, sites that indicate prejudice against a certain religion, race, nationality, gender, age, disability, or sexual orientation, or sites that contain descriptions or images of physical assaults against humans, animals, or institutions.

- Illegal downloads

For example, sites that provide illegal or questionable access to software, and sites that develop and distribute programs that may compromise networks and systems.

- Anonymizers

For example, sites that attempt to make activity on the Internet untraceable or provide information how to bypass filtering.

- Unknown

If Parental control cannot retrieve the content type of the site, the site is categorized as unknown.

Selecting user's age group

With the age group, you can select who uses this device. Parental control limits the web content based on this selection.

To change the age group of the user:

1. In the main view, open **Parental control**.
2. In the **Parental control** menu, select **Settings**.
3. Turn on **Parental control** to blocks access to unwanted web pages.
4. In **Age group**, select who uses this device. Parental control limits the web content based on this selection. Changing the age group changes the categories that the user is allowed to browse.
5. To view and edit blocked categories, select **Options** > **Edit profile**.
6. Select which categories you want to block.

After you have changed the age group, Parental control allows access only to web sites that you have configured.

Keeping the application up-to-date

The automatic update service in the product checks for new updates regularly and keeps the product up-to-date.

After you activate the product, automatic updates is turned on. Automatic updates require an active Internet connection. When a connection to the Internet is available, the product checks for updates regularly and downloads new updates if necessary.

Only an up-to-date virus definition database protects your device against the latest viruses.



Note: You can freely update the product as long as you have an active subscription. To keep your device continuously protected, purchase additional service time well before the expiration date.

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. Browse to **Settings** and press the selection key.
The settings selection list opens.
2. Select **Virus protection** from 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. (recommended)
 - **In home network** – the application downloads updates from the update server automatically when you are using your own operator's network.
 - **Never** – the virus definitions are not updated automatically. We do not recommend that you disable automatic updates.

Manual updates

You can update the product manually any time you want.


To update the product manually, follow these instructions:

1. In any of the main views, press **Options > Update**.
The product needs to connect to the Internet to check for the latest updates.
2. Select the Internet access point to connect to the update server.
For more information, see the User Guide of your device.
The application downloads the latest virus definition database and takes it into use immediately.
3. When the update is complete, press **OK** to scan your device for viruses.

Application updates

When a new product version is available, a message asks you to download it.

The application restarts automatically when the update is completed.

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

Upgrading the application manually

You can upgrade the product by installing the latest version.

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 the latest version of the product.
5. Activate the new version with your key code.

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.

The product supports several purchase methods depending on the distribution channel. Most common purchase methods are:

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

If you wish to purchase the product after using the trial version, use the subscription number 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.

Purchasing subscription service time with SMS

You can purchase more service subscription time with SMS text message.

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

1. Browse to **Buy** and press the selection key.
The **Select method** screen is displayed.
2. Select the **Phone bill** payment method.
3. When prompted to accept payment, press **OK** to complete your subscription service time purchase.
4. In the response SMS, you receive a confirmation of your purchase and a code for activating the service.

Purchasing subscription service time with credit card

You can purchase more service subscription time with your credit card.

To purchase more subscription service time using the application, follow these instructions:

1. Browse to **Buy** and press the selection key.
The **Select method** screen is displayed.
2. Select **Buy with credit card**.
If you have a license already, you can activate the service with your license code.
3. The application open the link to the F-Secure eStore. Follow the on-screen instructions to finish the purchase.

Purchasing subscription service time with your PC

You can use your computer to purchase more service subscription time for the product.

To purchase more service subscription time with the web browser of your computer, follow these instructions:

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

Technical support

Topics:

- [Security overview](#)

Instructions how to check the current status of the application.

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.

Security overview

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