

F-Secure Mobile Security with Parental control

Android

Contents

Chapter 1: Installation.....	5
Installing.....	6
Activating.....	6
Configuring the product.....	7
Uninstalling the product from the Android device.....	7
Chapter 2: Protecting confidential information.....	9
Turning on remote Anti-Theft.....	10
Locking your device remotely.....	10
Wiping your device remotely.....	10
Locating your device.....	10
Using the SMS alert.....	11
Using Anti-Theft alarm.....	11
Using location sharing.....	11
Chapter 3: Protecting web browsing.....	13
Using Browsing protection.....	14
Changing the default browser.....	14
Using the Internet safely.....	14
Changing the Browsing protection settings.....	14
Chapter 4: Scanning for viruses.....	17
Manual scanning.....	18
Processing infected files.....	18
Changing the virus protection settings.....	18
Chapter 5: Making browsing safe for children.....	19
What are age groups.....	20
Content types.....	20
Selecting user's age group.....	21
Using Application control.....	21
Chapter 6: Preventing unwanted calls and messages.....	23
Using Safe contacts.....	24
Viewing blocked calls and messages.....	24

Chapter 7: Keeping the application up-to-date.....	25
Selecting the update mode.....	26
Manual updates.....	26
Chapter 8: Purchasing subscription service time.....	27
Purchasing subscription service time with your PC.....	28

Installation

Topics:

- [Installing](#)
- [Activating](#)
- [Configuring the product](#)
- [Uninstalling the product from the Android device](#)

Instructions how to install the product on the mobile device.

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

- Download the installation file to your computer and move it to the device or SD card, or
- Download the installation file directly to your device.

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

Installing

Instructions how to install the product on the mobile device.

If you are upgrading from a previous version of the product, you do not need to uninstall the previous version, but check the product settings after you have installed the new version.

Follow these instructions to install the product:

1. Open **Settings** > **Application** and check that **Unknown sources** is turned on.

When this setting is turned on, you can install applications outside the Android Market.

2. Download the installation file to your computer and move it to the device or SD card, or download the installation file directly to your device.

For more information, consult the documentation that came with your device.

3. Launch the installation package on your device to install the product.

Note that you need a third-party file manager to launch the installation package from the memory card.

The installation package installs the product to your device.

4. After the installation is complete, choose **Open** to start the application and to activate the product.

The product does not protect your device before you activate 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 **OK** after you accept them.


The activation starts after you have accepted the license terms.

3. Select the activation type.

You can activate the product either in the free trial mode or with your subscription code. Depending on the license type you have purchased, you can use either Anti-theft or Mobile Security with Browsing protection.

- To evaluate the product, select **Free Trial** as the activation type.
- If you already have a subscription key, select **Subscription key** as the subscription type and enter your subscription key.

4. Press **Activate**.

 **Note:** The product needs to connect to the update service during the activation.

After you have finished the activation, the configuration wizard opens where you can set up the product.

On Android 2.2 and later platforms, you need to activate the device administrator for the product to use Anti-Theft.

Configuring the product

You need to configure the product features before you can use it.

Follow these instructions to take Anti-Theft, Parental control and Safe contacts features into use:

1. Enter new security code and verify it to make sure you entered it properly.

 **Note:** To change the security code later, open [Settings](#) > [General settings](#) and select [Set security code](#).

You need the security code to use remote Anti-Theft features and to use Parental control.

2. The product requires rights to administer your device. To activate the device administrator, press [Activate](#).
3. If you have not set the screen lock for your device, you need to do so before you can continue.
For more information, consult the documentation that came with your device.

4. Enter the trusted phone number.

The trusted phone number receives alerts when the SIM card is changed in your device.

5. Select the age group of the user of the device to configure the Parental Control.

After you have configured Anti-Theft and Parental Control, the product is turned on.

Uninstalling the product from the Android device


Instructions how to remove the product from your device.

To uninstall the product from your device, follow these instructions:

1. In the main view, open [Settings](#).
2. In the [Settings](#) menu, select [General](#).
3. Tap [Uninstall](#).

If you have created a security code for Anti-Theft, you need to enter it to uninstall the product.

The product is removed from your device.

 **Note:** The product is deactivated in the [Device administrator](#) list during the uninstallation. If you cancel the uninstallation, you need to activate the product again to continue to use it.

Protecting confidential information


Topics:

- [Turning on remote Anti-Theft](#)
- [Using the SMS alert](#)
- [Using Anti-Theft alarm](#)
- [Using location sharing](#)

With Anti-Theft, you can make sure that your device or data stored on it is not misused if your device is stolen.

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 screen unlock pattern.

 **Note:** To use the remote lock, keep the screen unlock pattern of your device 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 removes information in the inserted SD card, SMS and MMS messages, contacts and calendar information. In addition, we recommend that you change the password of your Google account.
- On Android 2.2 and later platforms, the product resets the device to factory defaults when you send an SMS message to wipe your device.

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 locate your device remotely, select **Enable locator**.

To use the locator, 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.

4. Select **Remote Anti-Theft** to turn it on.

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:

1. To lock the device, send the following SMS message to your device: #LOCK#<security code>
(For example: #LOCK#12345678)
2. When the device is locked, the product sends a reply message to the phone that you used to sent the lock message. If you have turned on the remote locate, the reply contains the location information of the device.

Locked device can be unlocked only with the screen unlock method that you have selected.

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:

1. To wipe the device, send the following SMS message to your device: #WIPE#<security code>
(For example: #WIPE#12345678)
2. When the device is wiped, the product sends a reply message to the phone that you used to sent the wipe message.

When you wipe the device, the product removes information in the inserted SD card, SMS and MMS messages and contacts and calendar information. On Android 2.2 and later platforms, wiping the device resets it to factory defaults.

Locating your device



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

 **Note:** Make sure that you have turned on GPS in your device to receive the location information.

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 **Trusted 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.


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 sent the alarm message.

To turn off the alarm, use the screen unlock method that you have selected.

-  **Tip:** You can turn off the alarm remotely by sending the following SMS message to your device: #ALARM#<security code>#0

Using location sharing

You can send a message to your friends and family that displays your current location on the map.

You need to have turned on the GPS in your device to share your location.

To send the location sharing message:

1. In the main view, open **Anti-Theft**.
2. In the **Anti-Theft** menu, select **Location sharing**.
The product uses the GPS to retrieve your location and opens the messaging application.
3. In the messaging application, add recipients for the location information message and press **Send**.
The message contains information of your location and a link to Google Maps that points where you are.

Protecting web browsing

Topics:

- [Using Browsing protection](#)
- [Using the Internet safely](#)

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.

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. In the main view, select **Settings**.
2. Select **Browsing protection**.
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.


Scanning for viruses

Topics:

- [Manual scanning](#)
- [Processing infected files](#)
- [Changing the virus protection settings](#)

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

The product scans installed programs and inserted memory cards for viruses, spyware and riskware automatically.

 **Note:** We recommend that you scan your device for viruses whenever the product asks you to do so.

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. In the main view, select **Virus protection**.
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.

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. In the main view, select **Virus protection**.
2. Select **Infected files**.
The **Infected files view** opens.
3. In the **Infected files view**, scroll to the infected file you want to process.
4. Select the infected file to view more details about it. The **Infected files details view** displays the path and file name of the infected file, and the name of the infection.
5. Select **Delete** or **Uninstall** to remove the infected file or application from your device.

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/>.

Changing the virus protection settings

Change the virus protection settings to select when you want to run the virus scan.

To change the virus protection settings, follow these instructions:

1. In the main view, select **Settings**.
The settings selection list opens.
2. Select **Virus protection** from the settings selection list.
3. Select **Installation scan** to scan any program automatically after you install it to your device.
4. Select **Memory card scan** to scan a memory card automatically every time you insert it into your device.

Making browsing safe for children

Topics:

- [What are age groups](#)
- [Selecting user's age group](#)
- [Using Application control](#)

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.

What are age groups

With age groups, you can define web content that is 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, select **Settings**.
2. Select **Parental control**.
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 content that the user is allowed to browse.
5. To view and edit allowed categories, select **Restricted web content**.
6. Select which content you want to allow.

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

Using Application control

With Application control, you can limit applications can be used and uninstall any unwanted applications.

Parental control needs to be turned on to use Application control.

To use Application control, follow these instructions:

1. In the main view, select **Settings**.
2. Select **Parental control**.
3. Turn on **Parental control**.

4. Turn on **Application control**.
5. Select **Restricted applications**.
Parental control displays a list of installed applications
6. To allow the user of the device to use the application, make sure the check box next to the application is checked. To restrict the access to the application, clear the check box.
By default, Parental control allows access to all applications.
7. If you want to remove an application from the device completely, press and hold the application in the list until you see the uninstall prompt. Select **Uninstall** to remove the application.

When anyone tries to open an application that you block with Application control, a block page opens and the Parental control denies the access to the application.

Preventing unwanted calls and messages

Topics:

- [Using Safe contacts](#)
- [Viewing blocked calls and messages](#)

Safe contacts prevents unwanted calls and messages from reaching you.

With Safe contacts, you can focus on calls and messages that matter to you and block unwanted calls and spam messages.

You can choose numbers that you want to block and Safe contacts blocks all incoming calls and SMS/MMS messages from the numbers that you choose. Safe contacts restricts outgoing calls to numbers on the block list as well.

Using Safe contacts

Safe contacts blocks calls and messages from numbers in the block list.

To block calls and messages from a new number, follow these instructions:

1. In the main view, select **Settings**.
The settings selection list opens.
2. Select **Safe contacts** from the settings selection list.

 **Note:** You need to set up your security code if you have not done that yet.

3. Make sure that **Safe contacts** is turned on.
4. Select **Block numbers**.
You need to enter your security code to block new numbers.
The blocked numbers list opens.
5. Select **Enter a number to block**.
6. Enter the name and number that you want to block.
7. Select **Save** to add the number to the blocked numbers list.

When the Safe contacts is turned on, you do not receive any calls or messages from the numbers in the blocked numbers list and all calls to blocked numbers are restricted as well.

Viewing blocked calls and messages

You can see in which calls and messages Safe contacts has blocked in the block history.

To view which calls and messages Safe contacts has blocked, follow these instructions:

1. In the main view, select **Settings**.
The settings selection list opens.
2. Select **Safe contacts** from the settings selection list.
3. Select **Show block history**.


Keeping the application up-to-date

Topics:

- [Selecting the update mode](#)
- [Manual updates](#)

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.

 **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:

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 the main view, select **Update**.
The product needs to connect to the Internet to check for the latest updates.
2. Select **Yes** to check for the latest updates.
If a new update is available, the product asks you to download it.
3. If a new update is available, select **Yes** to download the software update.
4. When the download is complete, select **Install** to install the update.

Purchasing subscription service time

Topics:

- [Purchasing subscription service time with your PC](#)

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

If you wish to purchase F-Secure Mobile Security after using the trial version, or you want to upgrade F-Secure Anti-Theft to F-Secure Mobile Security, use the **Buy** menu in the application.

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.