# ESET Mobile Security

## for Symbian

Installation Manual and User Guide - Public Beta

# ESET Mobile Security



Customer Care Worldwide: www.eset.eu/support
Customer Care North America: www.eset.com/support

REV. 25. 3. 2010

## Contents

# 1. Installation of ESET Mobile Security

## 1.1 Minimum system requirements

To install ESET Mobile Security for Symbian, your mobile device must meet following system requirements:

| | Minimum system requirements |
|---|---|
| Operating system | S60 3rd Edition Feature Pack 1 or 2<br>S60 5th Edition |
| Available free space | 2 MB |

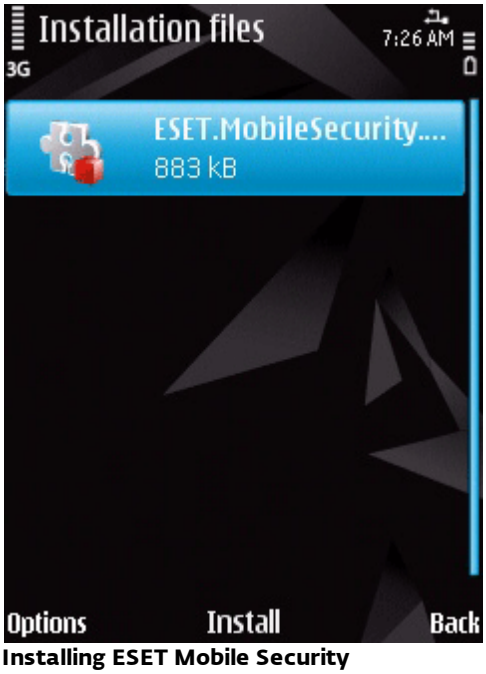
## 1.2 Installation

Save all open documents and exit all running applications before installing. You can install ESET Mobile Security directly on your device or use your computer to install it.

After successful installation, activate ESET Mobile Security by following the steps in the Product activation 5 section.

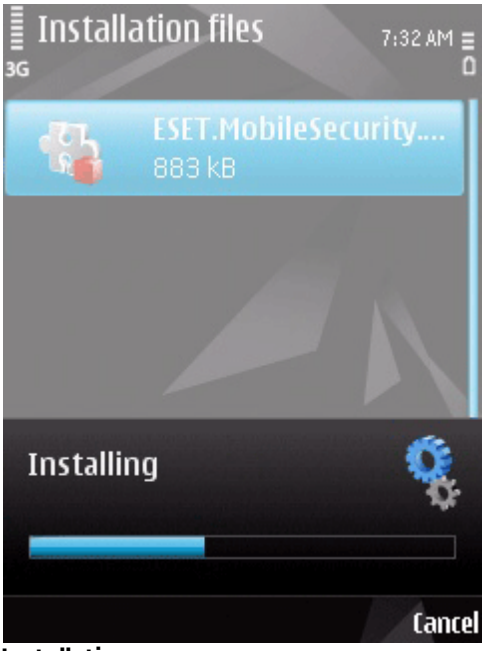
### 1.2.1 Installation on your device

To install ESET Mobile Security directly on your device, download the *.sisx* installation file onto your device by Wi-Fi, Bluetooth file transfer or email attachment. Locate the file on your device. Tap the file to launch the installer and then follow the prompts in the installation wizard.




**Installing ESET Mobile Security**

**NOTE:** The Symbian user interface varies by device model. The installation file may appear in a different menu or folder on your device.

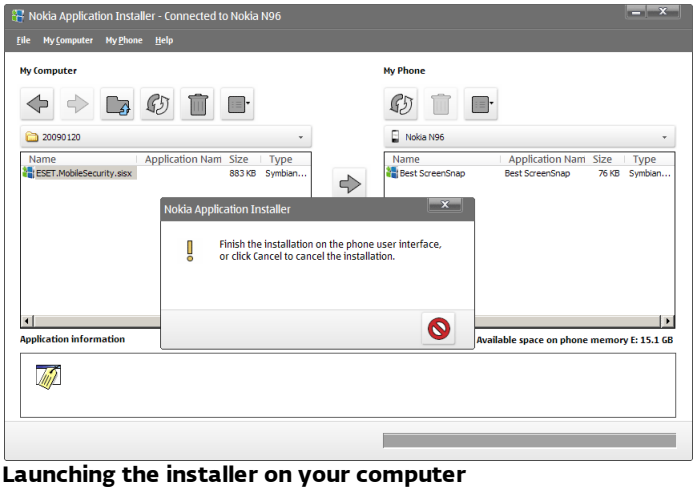



**Installation progress**

After installation, you can modify the program settings. However, the default configuration provides the maximum level of protection against malicious programs.

### 1.2.2 Installation using your computer

To install ESET Mobile Security using your computer (via Nokia PC Suite in Microsoft Windows), please connect your mobile device to the computer. After the device is recognized, run the downloaded installation package (*.sisx* file) and follow the instructions in the installation wizard.



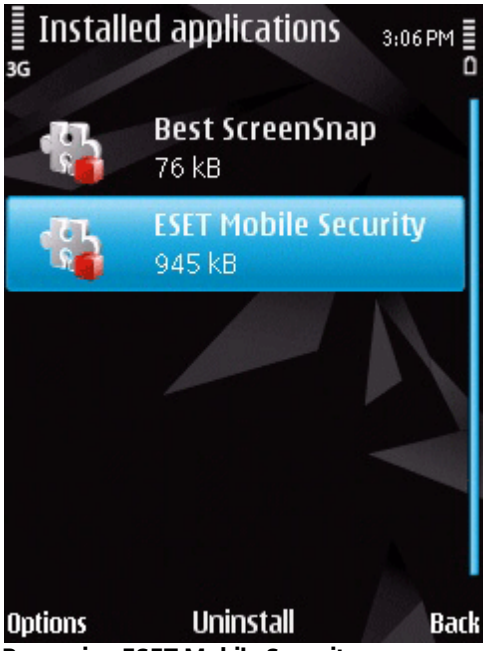

**Launching the installer on your computer**

Then follow the prompts on your mobile device.

## 1.3 Uninstallation

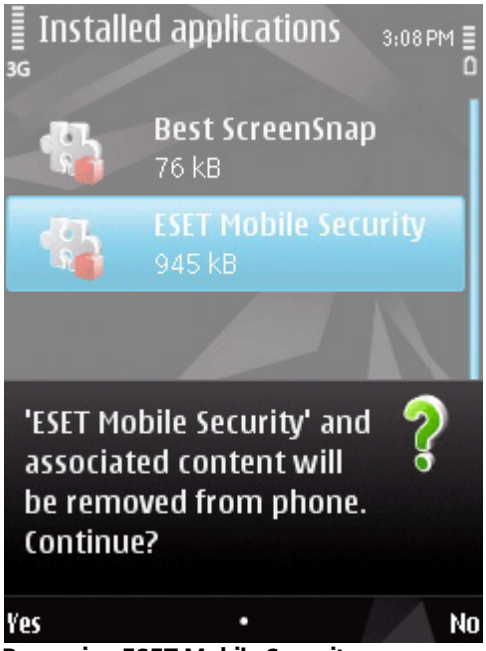
To uninstall ESET Mobile Security from your mobile device, tap **My Content > Application manager > Installed applications.**

**NOTE:** The Symbian user interface varies by device model. These options may be slightly different on your device.




**Removing ESET Mobile Security**

Select **ESET Mobile Security** and tap **Options > Uninstall**. Tap **Yes** when prompted to confirm the uninstallation.




**Removing ESET Mobile Security**

# 2. Product activation

The main ESET Mobile Security window (**My Content > Applications > ESET Mobile Security**) is the starting point for all instructions in this manual.


**The main ESET Mobile Security window**

After successful installation, ESET Mobile Security must be activated. If you are not prompted to activate your product, tap **Options > Activate.**


**Program activation**

There are two activation methods; the one that applies to you will depend on the manner in which you acquired your product.

## 2.1 Activation using username and password

If you purchased your product from a distributor, you received a username and password with your purchase. Select the **Login/Password** option and enter the information you received in the **Username** and **Password** fields. Enter your current contact address in the **Email** field. Tap **Options > Activate** to complete the activation.

## 2.2 Activation using registration key

If you acquired ESET Mobile Security with a new device (or as a boxed product), you received a Registration key with your purchase. Select the **Registration key** option, enter the information you received in the **Key** field and your current contact address in the **Email** field. Tap **Options > Activate** to complete the activation. Your new authentication data (Username and Password) will automatically replace the Registration key and will be sent to the email address you specified.

**NOTE:** During activation, the device must be connected to the Internet. A small amount of data will be downloaded. These transfers are charged according to your service agreement with your mobile provider.

# 3. Update

By default, ESET Mobile Security is installed with an update task to ensure that the program is updated regularly. You can also perform updates manually.

After installation, we recommend you run the first update manually. To do so, tap **Options > Action > Update.**

## 3.1 Settings

To configure update settings, tap **Options > Settings > Update.**

The **Internet Update** option enables or disables automatic updates. You can specify the **Update Server** from which updates are downloaded (we recommend leaving the default setting of *updmobile.eset.com*). In the **Login** and **Password** fields, enter the username and password you received after purchasing ESET Mobile Security. To set the time interval for the automatic updates, use the **Auto Update** option. In the **Default APN Connection** option, choose a type of connection that will be used for downloading updates.


**Update settings**

**NOTE:** To prevent unnecessary bandwidth usage, virus signature database updates are issued as needed, when a new threat is added. While virus signature database updates are free with your active license, you may be charged by your mobile service provider for data transfers.

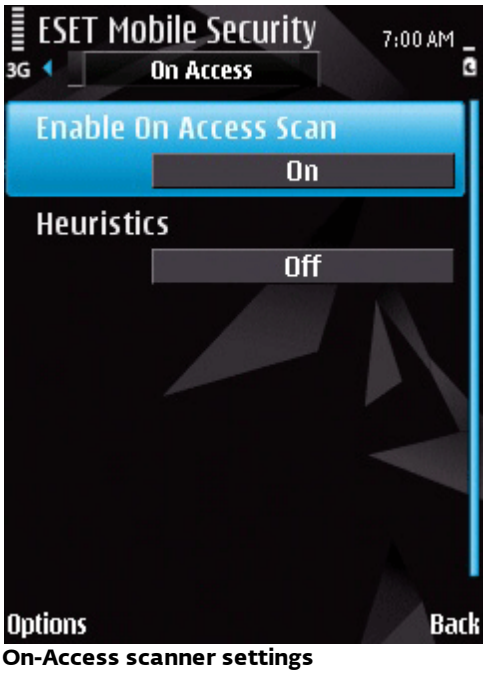
# 4. On-Access scanner

The On-Access scanner checks files that you interact with in real time. Files that are run, opened or saved are checked for viruses automatically. Scanning takes place before any action is performed on a file, ensuring maximum protection with default settings. The On-Access scanner launches automatically at system startup.

## 4.1 Settings

Tap **Options > Settings > On Access** to enable or disable following options:

- **Enable On Access Scan** – If selected, the On-access scanner runs in the background.
- **Heuristics** – Select this option to apply heuristic scanning techniques. Heuristics proactively identifies new malware not yet detected by the virus signature database by analyzing code and recognizing typical virus behavior. Its disadvantage is that additional time is required to complete the scan.




**On-Access scanner settings**

# 5. On-Demand scanner

You can use the On-Demand scanner to check your mobile device for the presence of infiltrations. Certain, predefined, file types are scanned by default.

## 5.1 Running a whole device scan

A whole device scan checks memory, running processes, their dependent dynamic link libraries (DLLs) and files that are part of internal and removable storage.

To run a whole device scan, tap **Options > Action > Scan device.**

**NOTE:** A memory scan is not performed by default. To activate it, tap **Options > Settings > General** and switch the **Memory Scan** option to **On.**


**Running a whole device scan**

The program scans system memory first (including running processes and their dependent DLLs) and then scans files and folders. The full path and file name of each scanned file will be displayed briefly.

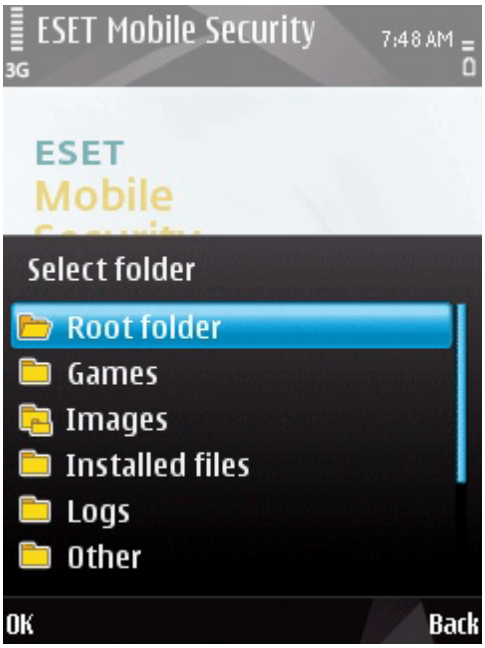
**NOTE:** To abort a scan in progress, tap **Cancel** in the bottom right corner.

## 5.2 Scanning a folder

To scan a particular folder on your device, tap **Options > Action > Scan folder.**


**Scanning a folder**

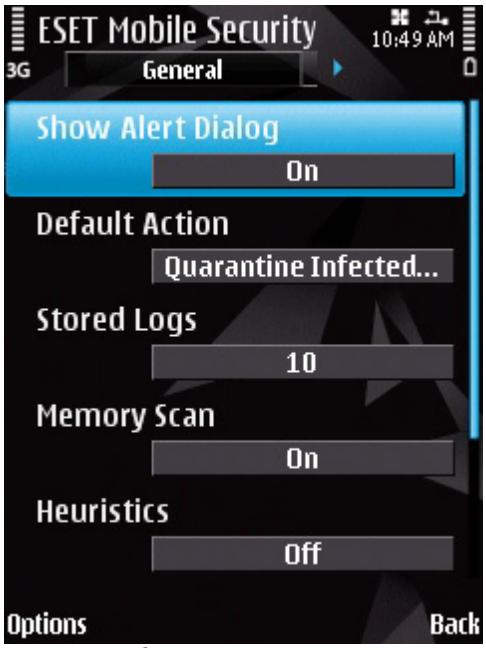
Select the memory of your device or memory card and then specify the folder you wish to scan.




**Selecting a folder to scan**

## 5.3 General settings

To modify scanning parameters, tap **Options > Settings > General.**




**General settings**

The **General** settings window allows you to specify which action to take if a virus is found. Switch the **Show Alert Dialog** option to **On** to display virus alert notifications.

The **Default Action** option allows you to select an action to be performed automatically for infected files. You can choose from the following options:

- **Quarantine Infected File**
- **Delete Infected File**
- **Do Nothing (not recommended)**

The **Stored Logs** option allows you to define the maximum number of logs to be stored in the **Options > Logs > Scan** section.

If the **Memory Scan** option is set to **On**, the device memory will be automatically scanned for malicious programs prior to the actual file scan.

If the **Heuristics** option is set to **On**, ESET Mobile Security will use heuristic scanning techniques. Heuristics is an algorithm-based detection method that analyzes code and searches for typical virus behavior. Its main advantage is the ability to identify malicious software not yet recognized in the current virus signature database. Its disadvantage is that additional time is required to complete the scan.

The **Archive Nesting** option allows you to specify the depth of nested archives to be scanned. (The higher the number, the deeper the scan.)

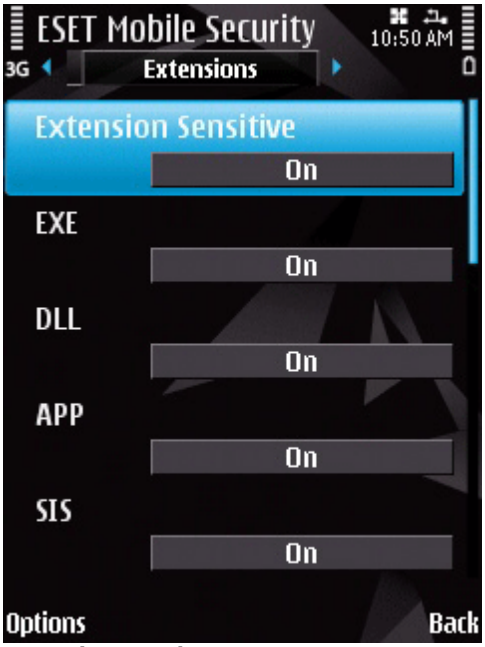
If the **Archive Deletion** option is set to **On**, archive files ( *zip*, *rar* and *jar*) containing infected objects, will be automatically deleted.

## 5.4 Extensions settings

To specify the file types to be scanned on your mobile device, tap **Options > Settings > Extensions.**

The **Extensions** window will be displayed, showing the most common file types exposed to infiltration. Select **On** for the file types you wish to scan or **Off** to exclude extensions from scanning. If you enable the **Archives** option, all supported archive files (*zip*, *rar* and *jar*) will be scanned.

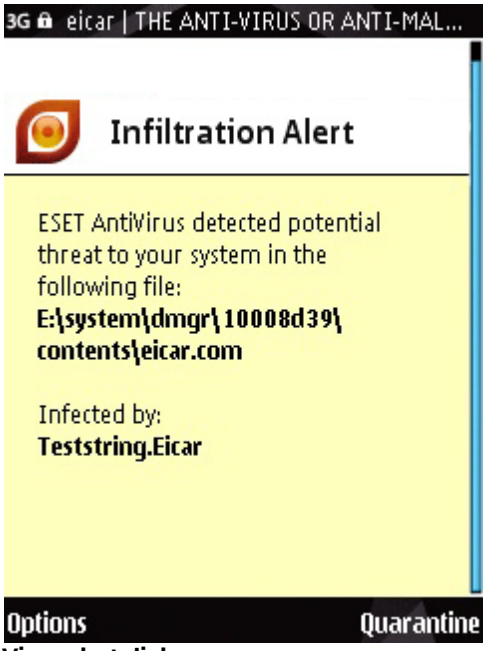
To scan all files, switch the **Extension Sensitive** option to **Off.**




**Extensions settings**

# 6. Virus found

If a virus is found, ESET Mobile Security will prompt you to take an action.




**Virus alert dialog**

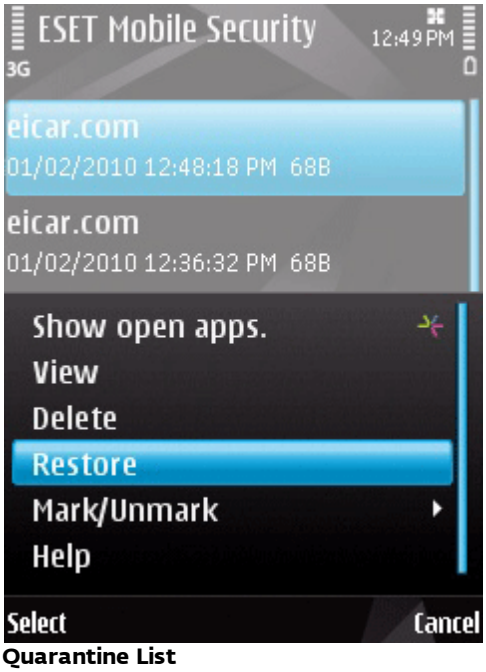
We recommend you select **Options > Delete**. If you select **Quarantine**, the file will be moved from its original location to quarantine. If you select **Options > Ignore**, no action will be performed and the infected file will remain on your mobile device.

If an infiltration is detected in an archive (e.g., *.zip* file), you can enable archive deletion by tapping **Options > Enable archive deletion** and then delete the archive ( **Options > Delete**).

## 6.1 Quarantine

The main task of the quarantine is to safely store infected files. Files should be quarantined if they cannot be cleaned, if it is not safe or advisable to delete them or if they are being falsely detected by ESET Mobile Security.

Files stored in the quarantine folder can be viewed in a log that displays the date and time of quarantine and original location of the infected file. To open quarantine, tap **Options > View > Quarantine List.**




**Quarantine List**

You can restore quarantined files by tapping **Options > Restore** (each file will be restored to its original location). If you wish to permanently remove the files, tap **Options > Delete**.

# 7. AntiTheft

AntiTheft protects your mobile phone from unauthorized access.

If someone steals your phone and replaces the SIM card with a new (untrusted) one, an Alert SMS will be secretly sent to certain phone number(s), which you can define. This message will include the phone number of the currently inserted SIM card, the IMSI (International Mobile Subscriber Identity) number and the phone's IMEI (International Mobile Equipment Identity) number. The unauthorized user will not be aware that this message has been sent, since it will be automatically deleted from the Sent folder.

To erase all data (contacts, messages, applications) stored on your device and all currently inserted removable media, you can send a Remote wipe SMS to the unauthorized user's mobile number in the form:
*#RC# DS password*
where *password* is your own password set in **Options > Settings > Password**.

## 7.1 Settings

First, set your password in **Options > Settings > Password**. This password is required for:
- sending a Remote wipe SMS to your device
- accessing the Anti Theft settings on your device
- uninstalling ESET Mobile Security from your device.


**Setting a security password**

To access AntiTheft settings, tap **Options > Settings > AntiTheft** and enter your password.

To disable automatic checking of inserted SIM card (and possible sending of Alert SMS), set **Enable SIM matching** to **Off**.

If the SIM card currently inserted in your mobile device is the one you wish to save as trusted, set the **Current SIM is trusted** option to **On.**.

If you are using more than one SIM card, you may want to distinguish each one by modifying its **SIM Alias** (e.g., *Office*, *Home* etc.).

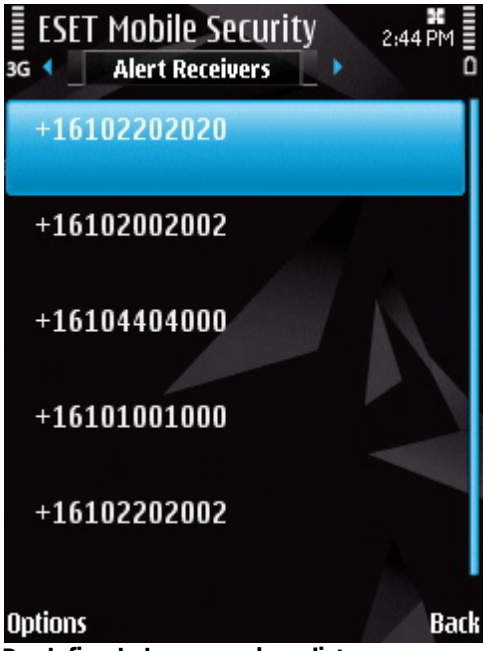
In **Alert SMS text**, you can modify the text message that will be sent to the predefined number(s) after an untrusted SIM card is inserted in your device.

The **Run after restart** option triggers automatic start-up of all AntiTheft features (Alert SMS, protection against uninstalling ESET Mobile Security etc.) and the On-Access scanner after each restart of the device. If this option is set to **Off,** the AntiTheft and On-Access will start only after you open ESET Mobile Security.


**Anti Theft settings**

The **Alert Receivers** tab shows the list of predefined numbers that will receive an Alert SMS after an untrusted SIM card is inserted in your device.To add a new number, tap **Options > Add**. To add a number from the contact list, tap **Options > Add from contact list.**

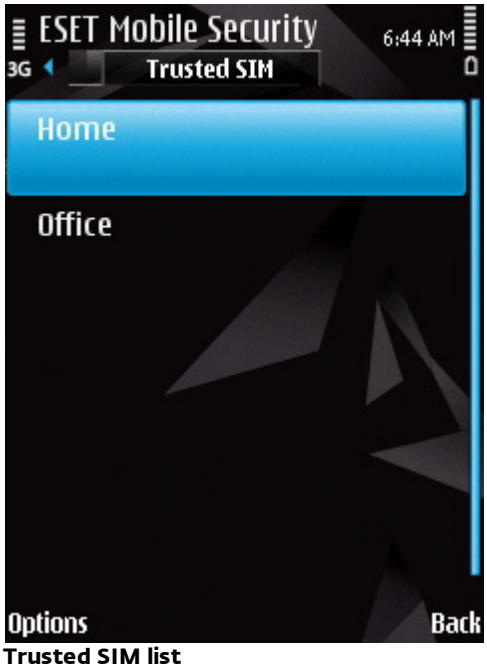
***Warning:*** the phone number must include the international dialing code followed by the actual number (e.g., *+16105552000*).




**Predefined phone numbers list**

The **Trusted SIM** tab shows the list of trusted SIM cards.

To remove a SIM from the list, select the SIM and tap **Options > Remove**.




**Trusted SIM list**

# 8. Firewall

The Firewall controls all inbound and outbound network traffic by allowing or denying individual connections based on filtering rules.

## 8.1 Settings

To modify the Firewall settings, tap **Options > Settings > Firewall.**


**Firewall settings**

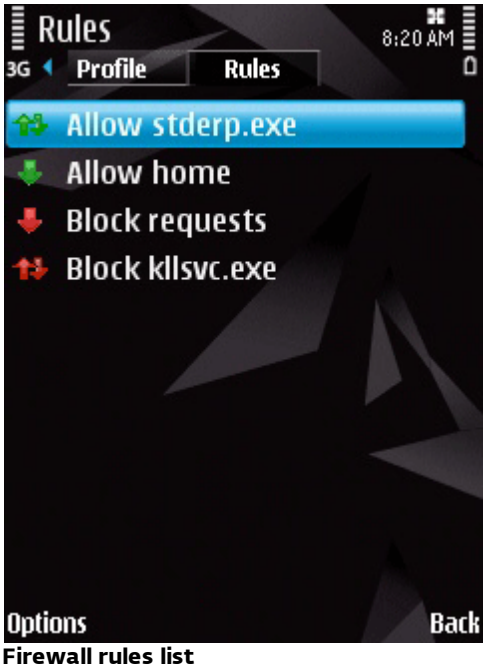
The **Start after reset** option lets you enable/disable firewall filtering after the phone restart.

Below you can choose from the following filtering modes:

- **Allow All -** allows all network traffic
- **Block All -** blocks all network traffic
- **Custom Rules -** lets you define your own filtering rules

While in **Custom Rules** mode, you can choose a default action for all inbound traffic (**Default Allow** or **Default Block**).

In the **Rules** tab, you can create, edit or remove filtering rules.




**Firewall rules list**

To create a new rule, tap **Options > New Rule** and fill in all the required fields.


**Creating a new rule**

# 9. Security audit

Security audit checks phone items such as battery level, bluetooth status, free disk space, etc.

To run security audit manually, tap **Options > Action > Run Security Audit.** A detailed report will be displayed.


**Security Audit results**

A green check next to each item indicates that the value is above the threshold or that the item does not represent a security risk. A red cross means that the value is below the threshold or that the item could represent a potential security risk.

If **Bluetooth status**, **IR status** or **Device visibility** is highlighted in red, you can turn off its status by selecting the item and tapping **Options > Fix**.

To see each item's details, select the item and tap **Options > Details**.

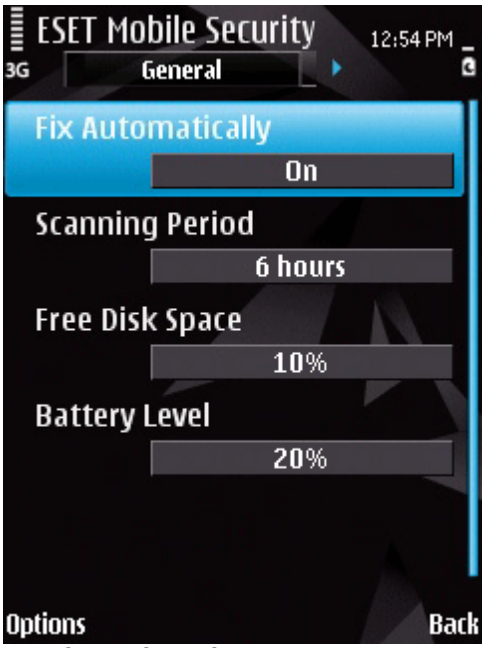

**Running Processes**

The **Running Processes** option shows the list of all processes running on your device.

To see the process details (full path name of the process, process UID and its memory usage), select the process and tap **Options > Details.**

## 9.1 Settings

To modify Security Audit parameters, tap **Options > Settings > SA Settings.**




**Security audit settings**

If the **Fix Automatically** option is set to **On**, ESET Mobile Security will automatically attempt to fix the items at risk (e.g., bluetooth status, device visibility) without user interaction. This setting only applies to an automatic (scheduled) audit.

The **Scanning Period** option allows you to choose how often the automatic audit will be performed. If you wish to disable the automatic audit, select **Never**.

Below you can adjust the threshold value at which the **Free Disk Space** and **Battery Level** will be considered as low.

In the **Test switches** tab, you can select the items to be checked during the automatic (scheduled) security audit.


**Automatic audit settings**

# 10. AntiSpam

AntiSpam blocks unsolicited SMS and MMS messages sent to your mobile device.

Unsolicited messages usually include advertisements from mobile phone service providers or messages from unknown or unspecified users.

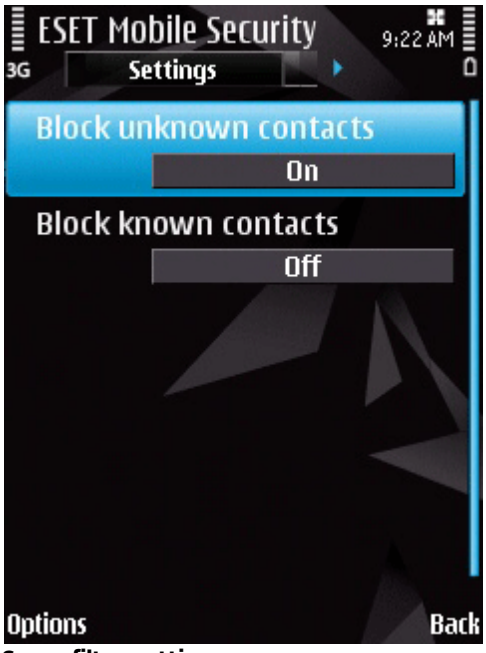
## 10.1 Settings

Tap **Options > View > Statistics** to see statistical information about received and blocked messages.

In the AntiSpam settings (**Options > Settings > AntiSpam**), the following filtering modes are available:

- **Block unknown contacts** – Enable this option to accept messages only from contacts in your address book.
- **Block known contacts** – Enable this option to allow messages only from senders not included in your address book.
- Set both **Block unknown contacts** and **Block known contacts** to **On** to automatically block all incoming messages.
- Set both **Block unknown contacts** and **Block known contacts** to **Off** to disable the AntiSpam. All incoming messages will be accepted.

**NOTE:** The Whitelist and Blacklist entries override these options (see Whitelist / Blacklist 16 section).

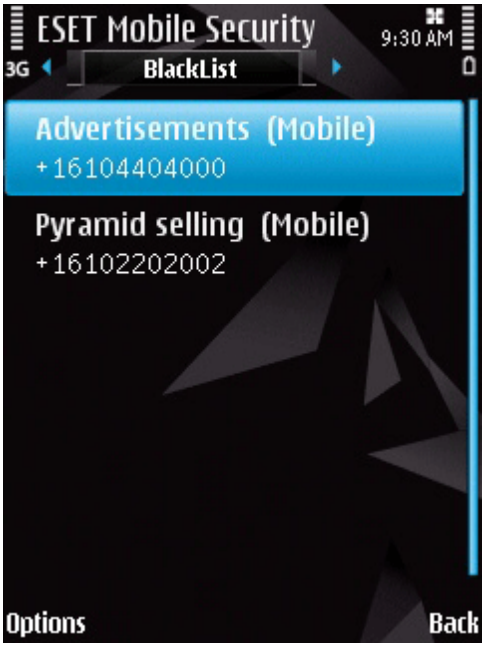



**Spam filter settings**

## 10.2 Whitelist / Blacklist

The **Blacklist** is a list of phone numbers from which all messages are blocked. Entries listed here override all options in the general spam filter setup (**Settings** tab).

The **Whitelist** is a list of phone numbers from which all messages are accepted. Entries listed here override all options in the general spam filter setup (**Settings** tab).



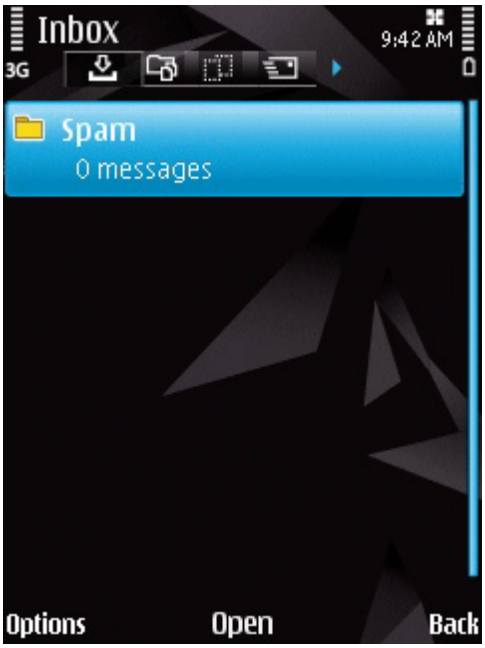

**Blacklist**

To add a new number to the Whitelist/Blacklist, select the tab for the list you wish to modify and tap **Options > Add.** To add a number from the contact list, tap **Options > Add contact.**

***Warning:*** Adding a number/contact to the blacklist will automatically and silently move messages from that sender to the **Spam** folder.

## 10.3 Locating spam messages

The **Spam** folder is used to store blocked messages categorized as spam according to the AntiSpam settings. To locate the **Spam** folder and review blocked messages, tap **Menu > Messaging > Inbox**.

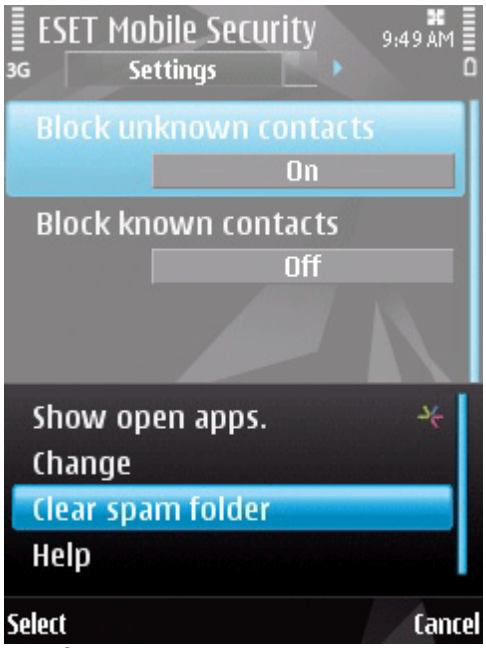



**Spam folder**

## 10.4 Deleting spam messages

To delete spam messages from your mobile device, follow the steps below:

1. Tap **Options > Settings > AntiSpam** from the ESET Mobile Security main window.
2. Tap **Options > Clear spam folder**.
3. Tap **Yes** to confirm the deletion of all spam messages.



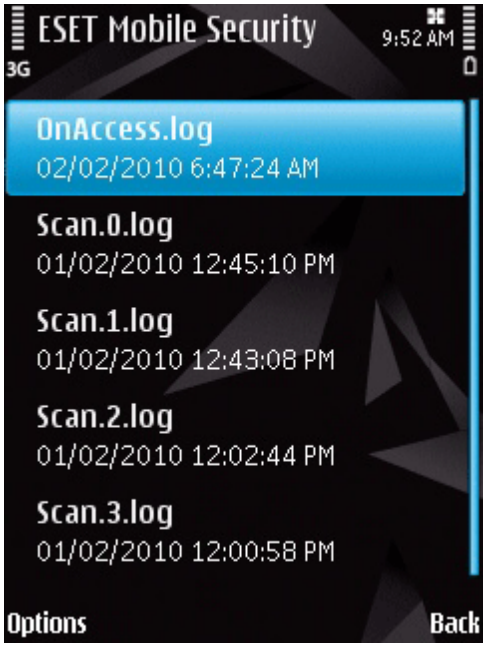

**Deleting Spam messages**

# 11. Viewing logs and statistics

The **Scan** log section (**Options > Logs > Scan**) contains logs providing comprehensive data about completed scan tasks. Logs are created after each accomplished On-Demand scan or when an infiltration is detected by the On-Access scan. All infected files are highlighted in red. At the end of each log entry is a reason the file is included in the log.

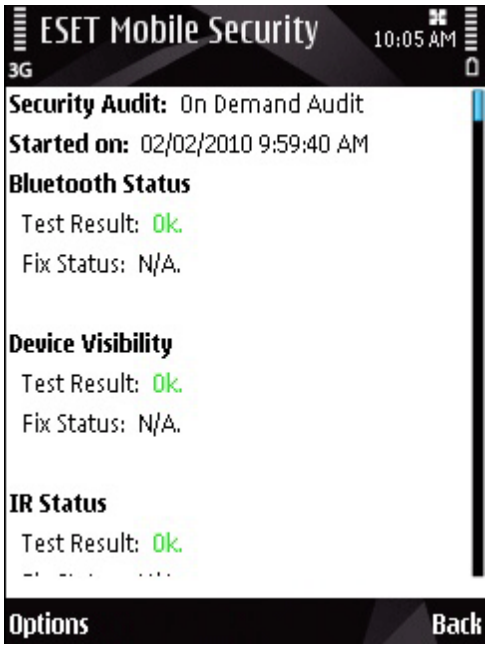
Logs contain:

- Log file name (usually in the form *Scan.Number.log*)
- Date and time of the event
- List of scanned files
- Actions performed or errors encountered during the scan




**Scan logs**

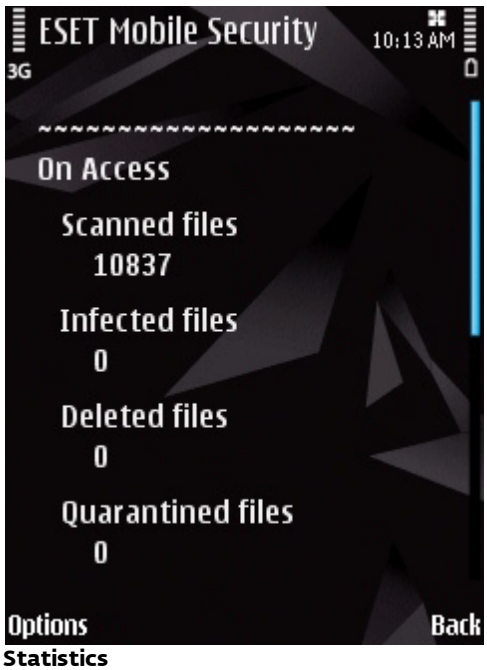
The **Security Audit** log section (**Options > Logs > SA Log** ) stores detailed results of the latest security audit.




**Security audit logs**

The **Statistics** screen (**Options > View > Statistics**) displays a summary of files scanned by the On-Access scanner and received/blocked messages.

If you wish to reset current statistics, tap **Options > Reset statistics**.




**Statistics**

# 12. Troubleshooting

This section provides solutions to common questions related to ESET Mobile Security.

## 12.1 Unsuccessful installation

The most common cause of an error message displayed during installation is that the wrong version of ESET Mobile Security has been installed on your device. When downloading the installation file from the *ESET homepage*, please make sure you are downloading the correct product version for your device.

## 12.2 Connection to update server failed

This error message is displayed after an unsuccessful update attempt if the program is not able to contact the update servers.

Try the following solutions:

1. Check your Internet connection – open your Internet browser to *http://www.eset.com* to verify that you are connected to the Internet
2. Verify that the program is using the correct update server – tap **Options > Settings > Update** and you should see *updmobile.eset.com* in the **Update Server** field.

## 12.3 Timeout downloading file

The Internet connection was unexpectedly slowed down or interrupted during the update. Try to run the update again later, please.

# 13. Technical support

For administrative assistance or technical support related to ESET Mobile Security or any other ESET security product, our Customer Care specialists are available to help. To find a solution to your technical support issue, you can choose from the following options:

To find answers to the most frequently asked questions, access the ESET Knowledgebase at:
*http://kb.eset.com*

The Knowledgebase contains an abundance of useful information for resolving the most common issues with categories and an advanced search.

To contact ESET Customer Care, use the support request form available at:
*http://eset.com/support/contact.php*