ESET Mobile Security

for Windows Mobile

Installation Manual and User Guide - Public Beta

ESET Mobile Security

Copyright © 2010 by ESET, spol. s.r.o.
ESET Mobile Security was developed by ESET, spol. s r.o.
For more information visit www.eset.com.
All rights reserved. No part of this documentation may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without permission in writing from the author.
ESET, spol. s r.o. reserves the right to change any of the described application software without prior notice.

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

REV. 9.4.2010

Contents

1. Installation of ESET Mobile Security 3
1.1 Minimum system requirements 3
1.2 Installation 3
1.2.1 Installation on your device 3
1.2.2 Installation using your computer 3
1.3 Uninstallation 4
2. Product activation 5
2.1 Activation using username and password 5
2.2 Activation using registration key 5
3. Update 6
3.1 Update using your computer 6
3.2 Settings 6
4. On-Access scanner 7
4.1 Settings 7
5. On-Demand scanner 8
5.1 Running a whole device scan 8
5.2 Scanning a folder 8
5.3 General settings 9
5.4 Extensions settings 9
6. Virus found 10
6.1 Quarantine 10
7. AntiTheft 11
7.1 Settings 11
8. Firewall 13
8.1 Settings 13
9. Security audit 14
9.1 Settings 14
10. Spam filter 16
10.1 Settings 16
10.2 Whitelist / Blacklist 16
10.3 Locating spam messages 16
10.4 Deleting spam messages 17
11. Viewing logs and statistics 18
12. Troubleshooting 20
12.1 Unsuccessful installation 20
12.2 Connection to update server failed 20
12.3 Timeout downloading file 20
12.4 Update file missing 20
13. Technical support 21

1. Installation of ESET Mobile Security

1.1 Minimum system requirements

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

	Minimum system requirements
Operating system	Windows Mobile 5.0 and later
Processor	200 MHz
Memory	16 MB
Available free space	2.5 MB

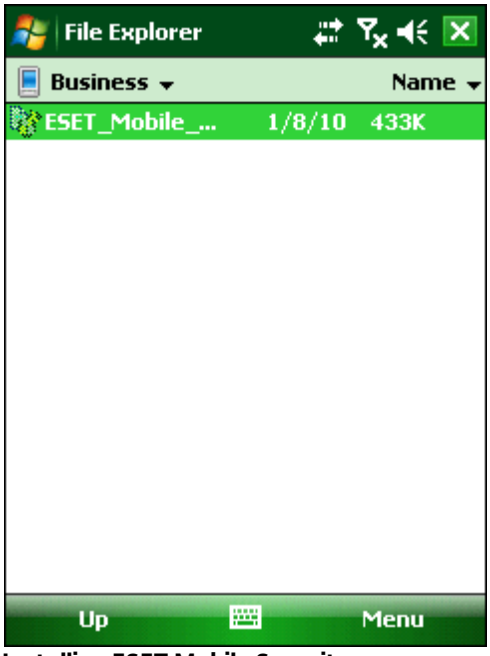
1.2 Installation

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.

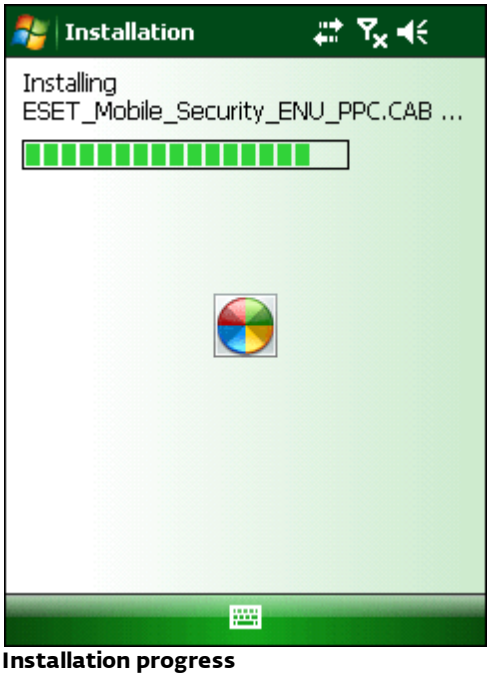
1.2.1 Installation on your device

To install ESET Mobile Security directly on your device, download the *.cab* installation file onto your device by Wi-Fi, Bluetooth file transfer or email attachment. Go to **Start > Programs > File Explorer** to locate the file. Tap the file to launch the installer and then follow the prompts in the installation wizard.



Installing ESET Mobile Security

NOTE: The Windows Mobile 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 Active Sync in Windows XP or Sync Center in Windows 7 and Vista), please connect your mobile device to the computer. After the device is recognized, run the downloaded installation package (*.exe* file) and follow the instructions in the installation wizard.

Launching the installer on your computer

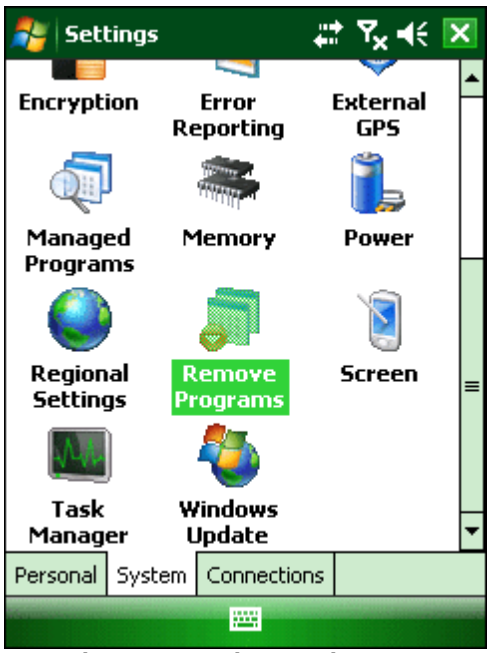
Then follow the prompts on your mobile device.

Warning: To successfully install your product using Windows Vista and Windows 7, you must be logged in as a user with admin privileges.

1.3 Uninstallation

To uninstall ESET Mobile Security from your mobile device, tap **Start > Settings**, tap the **System** tab and then tap the **Remove Programs** icon.

NOTE: The Windows Mobile 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 **Remove**. Tap **Yes** when prompted to confirm the uninstallation.

Removing ESET Mobile Security

2. Product activation

The main ESET Mobile Security window (**Start > Programs > 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 **Menu > 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 **e-mail** field. Tap **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 **e-mail** field. Tap **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 **Action > Update**.

3.1 Update using your computer

If your mobile device is not connected to the Internet, you can also update the virus signature database using your computer by following the steps below:

1. Disable the **Internet update** option in **Menu > Settings > Update**.
2. Download the file containing the most recent virus signature database to your PC.
3. Connect your device to your PC via Active Sync (in Windows XP) or Windows Mobile Device Center (in Windows Vista and Windows 7).
4. Copy the virus signature database update file (*EsetAV_WM.upd*) to the ESET Mobile Security installation directory (*Program Files\ESET\ESET Mobile Security*) on your device.
5. Tap **Action > Update** in the ESET Mobile Security main window. ESET Mobile Security will check the update file. If the file is not corrupted, the latest virus signature database will be installed.

3.2 Settings

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

The **Internet Update** option enables or disables automatic updates. You can specify the **Internet 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.

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.

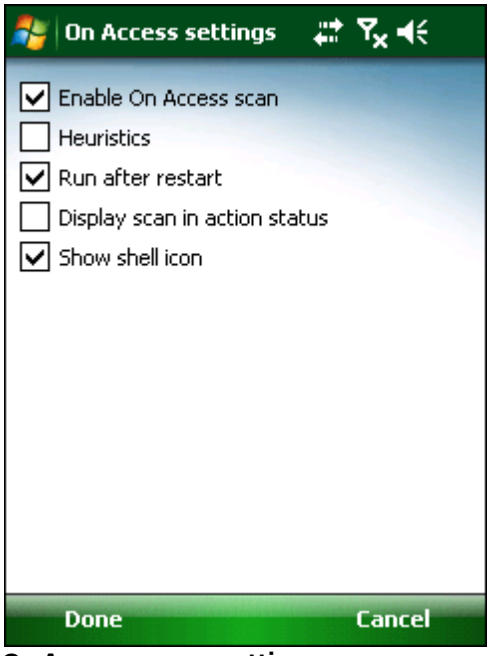
4. On-Access scanner

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 **Menu > 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.
- **Run After Restart** – If selected, the On-Access scanner will automatically start after restart of the device.
- **Display scan in action status** – Select this option to show scan status in the bottom right corner while scanning is in progress.
- **Show Shell Icon** – Displays the ESET Mobile Security icon on the main mobile device window.



On-Access scanner settings

5. On-Demand scanner

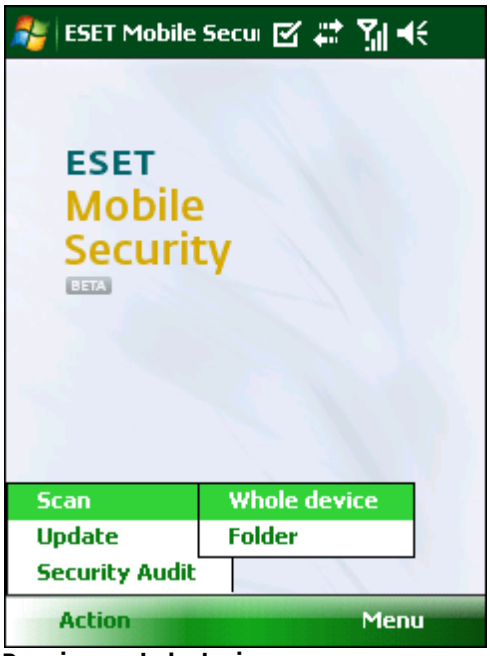
You can use the On-Demand scanner to check your mobile device for the presence of infiltrations. Certain, predefined, file types are scanned by default.

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 **Action > Scan > Whole device**.

NOTE: A memory scan is not performed by default. To activate it, tap **Menu > Settings > General** and select the **Memory Scan** check box.



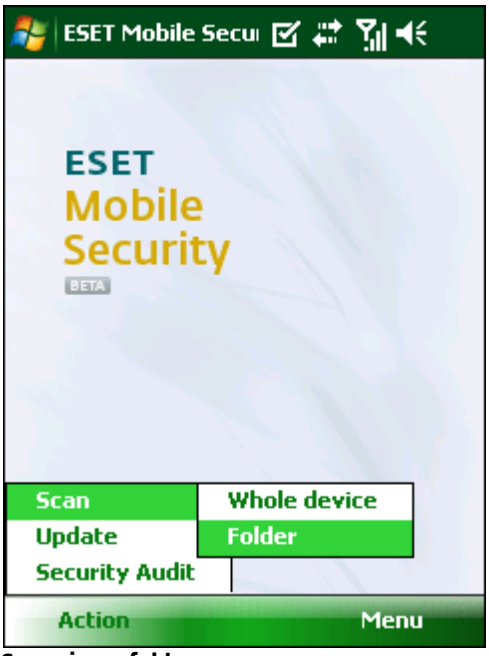
Running a whole device scan

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 **Action > Scan > Stop Scan.**

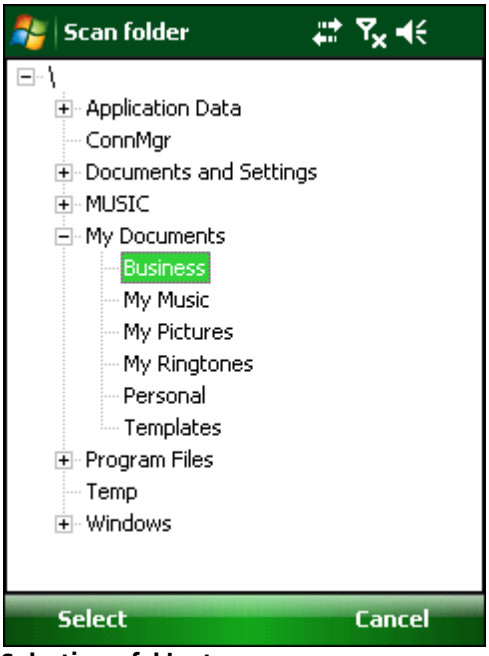
5.2 Scanning a folder

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



Scanning a folder

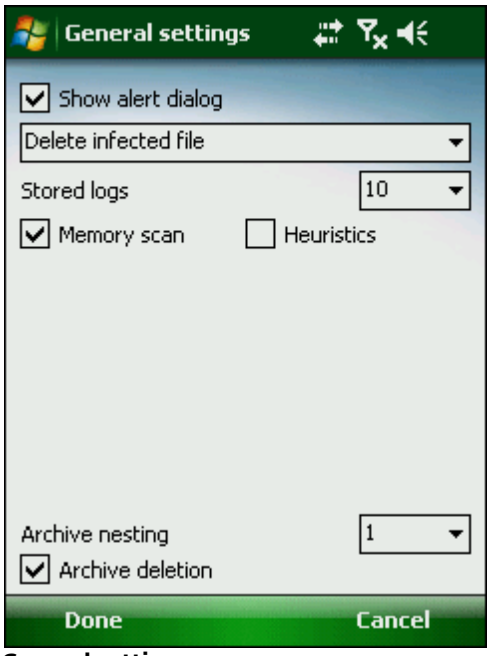
Tap the folder you wish to scan and tap **Select**.



Selecting a folder to scan

5.3 General settings

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



General settings

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

You can specify a default action that will be performed automatically for infected files. You can choose from the following options:

- **Move to quarantine**
- **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 **Menu > Logs > Scan** section.

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

If the **Heuristics** option is selected, 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 selected, 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 **Menu > Settings > Extensions.**

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

To scan all files, deselect the **Extension sensitive** checkbox.

Extensions settings

6. Virus found

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

Virus alert dialog

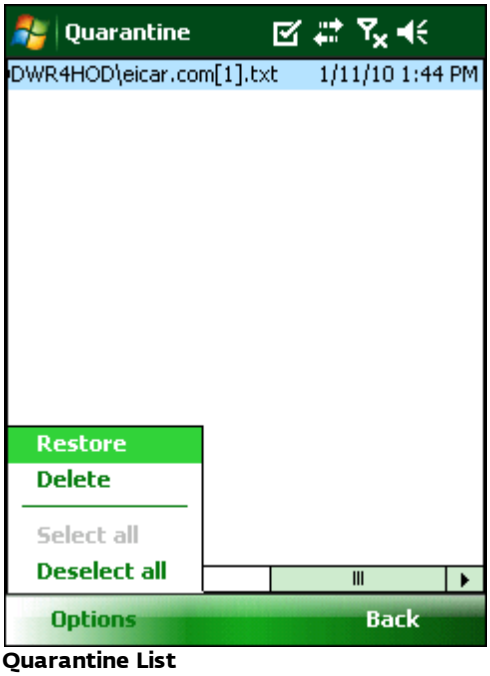
We recommend you select **Stop and delete**. If you select **Stop and move to quarantine**, the file will be moved from its original location to quarantine. If you select **Continue**, no action will be performed and the infected file will remain on your mobile device.

If an infiltration is detected in an archive (e.g., *.zip* file), the **Delete archive** option is available in the alert window. Select this option along with the **Delete infected file** option to delete all infected archive files.

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 **Menu > View > Quarantine.**



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.

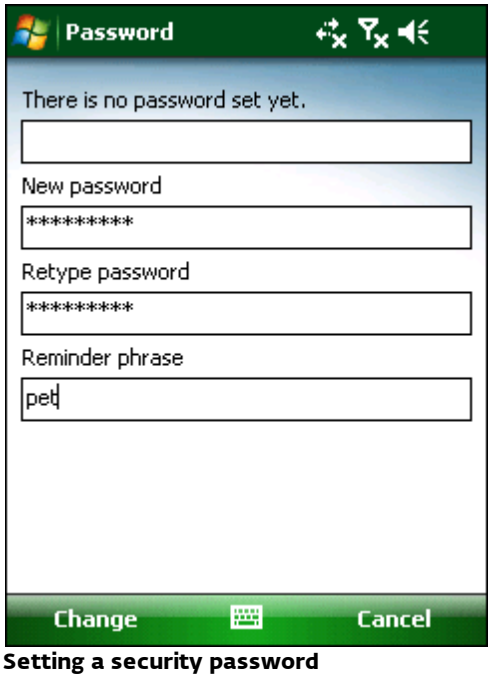
If someone steals your phone and replaces the SIM card with a new (untrusted) one, an Alert SMS will be secretly sent to certain phone number(s), which you can define. This message will include the phone number of the currently inserted SIM card, the IMSI (International Mobile Subscriber Identity) number 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 **Menu > Settings > Password**.

7.1 Settings

First, set your password in **Menu > 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

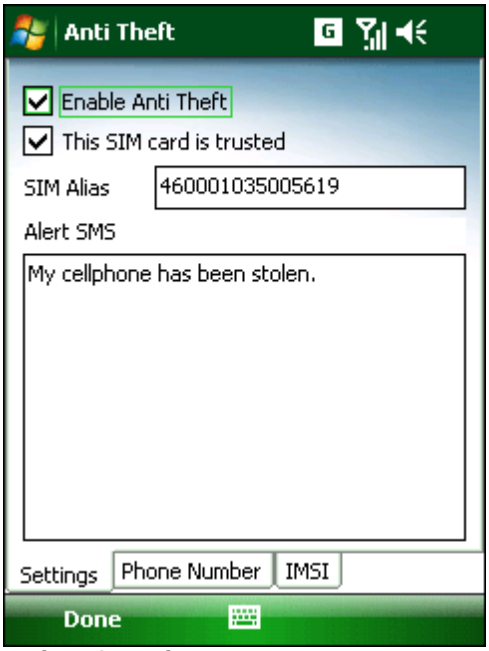
To access AntiTheft settings, tap **Menu > Settings > Anti Theft** and enter your password.

To switch Anti Theft on or off, select or deselect the **Enable Anti Theft** option.

If the SIM card currently inserted in your mobile device is the one you wish to save as trusted, check the **This SIM card is trusted** check box and the SIM will be saved to the Trusted SIM list (**IMSI** tab). The **SIM Alias** text box will be automatically filled with IMSI number.

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.).

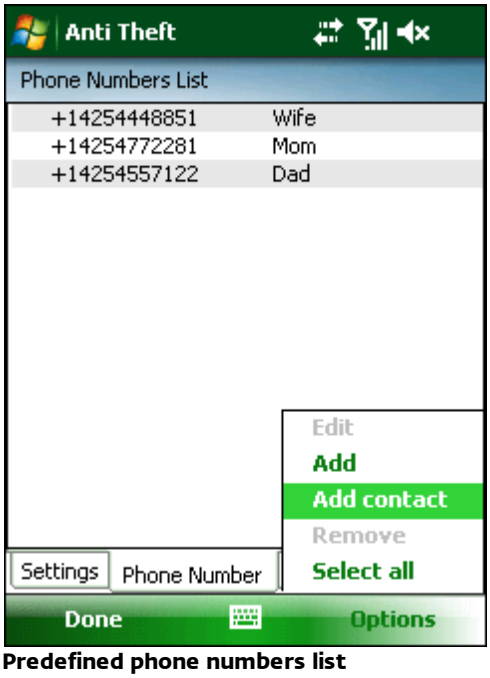
In **Alert SMS**, you can modify the text message that will be sent to the predefined number(s) after an untrusted SIM card is inserted in your device.



Anti Theft settings

The **Phone Number** 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 contact.**

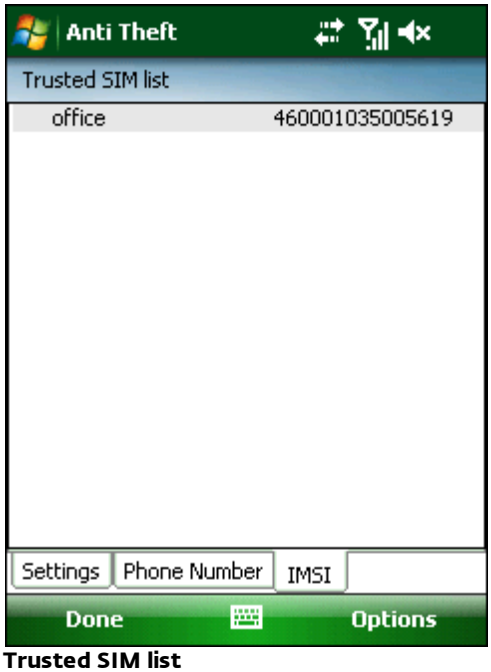
Warning: the phone number must include the international dialing code followed by the actual number (e.g., *+16105552000*).



Predefined phone numbers list

The **IMSI** tab shows the list of trusted SIM cards. Each entry consists of the SIM Alias (left column) and IMSI number (right column).

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



Trusted SIM list

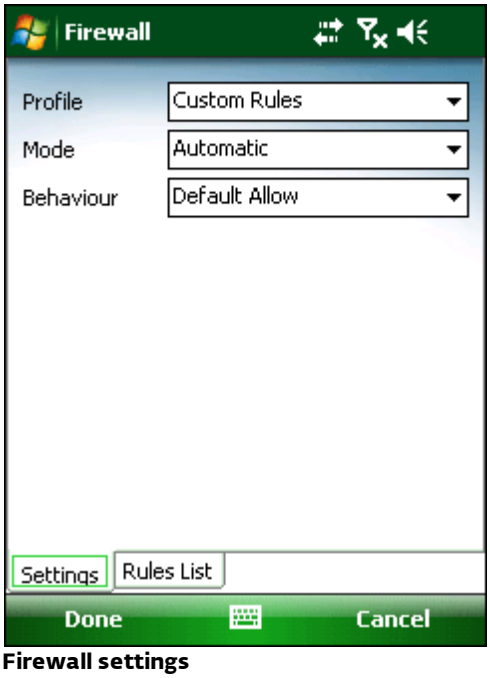
8. Firewall

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

Example of firewall alert dialog window

8.1 Settings

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



Firewall settings

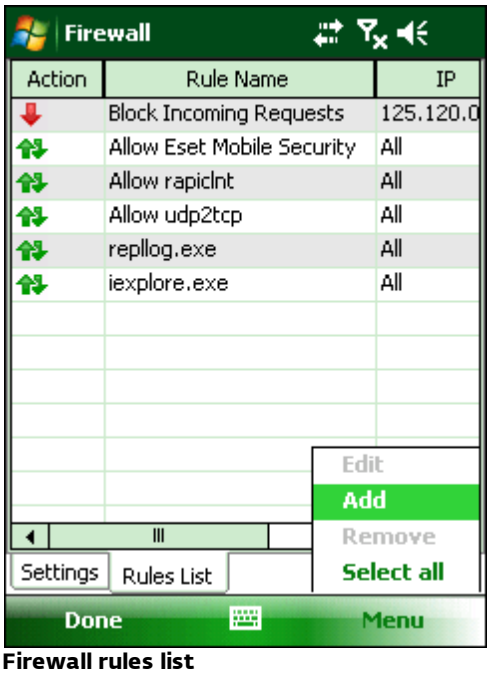
You can choose from the following profiles:

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

While in the **Custom Rules** profile, you can choose from two filtering modes:

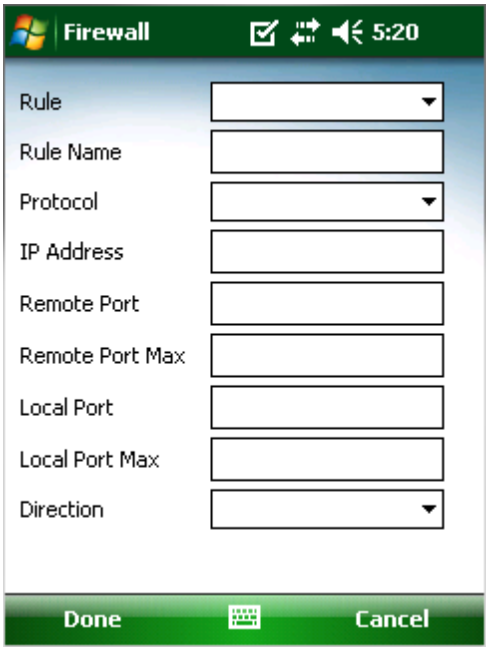
- **Automatic** - suitable for users who prefer easy and convenient use of the firewall with no need to define rules. This mode allows all outbound traffic. You can set a default action (**Default Allow** or **Default Block**) for inbound traffic .
- **Interactive** - allows you to customize your personal firewall. When a communication without a corresponding rule is detected, a dialog window reporting an unknown connection is displayed. The dialog window gives the option to allow or block the communication and to create a rule. If you choose to create a rule, all such future connections will be allowed or blocked according to the rule. If an application with an existing rule has been modified, a dialog window gives you the option to accept or deny this change. The existing rule will be modified based on your response.

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



Firewall rules list

To create a new rule, tap **Menu > Add**, fill in all the required fields and tap **Done**.

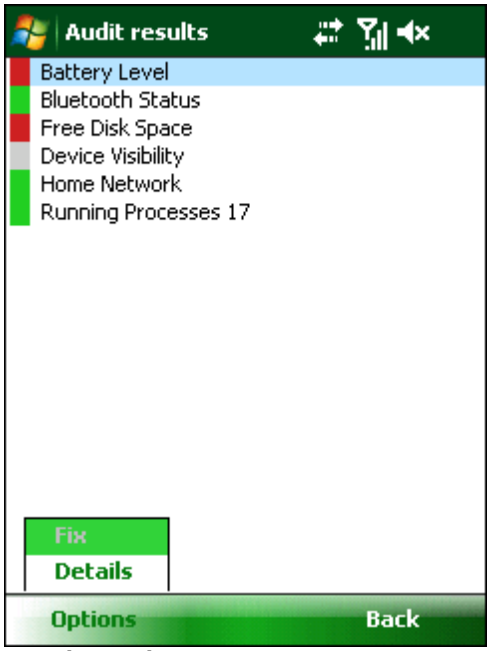


Creating a new rule

9. Security audit

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

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

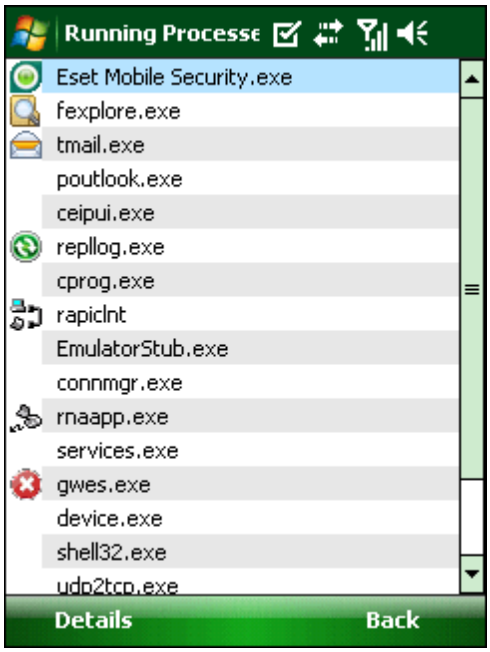


Security Audit results

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

If **Bluetooth 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**.



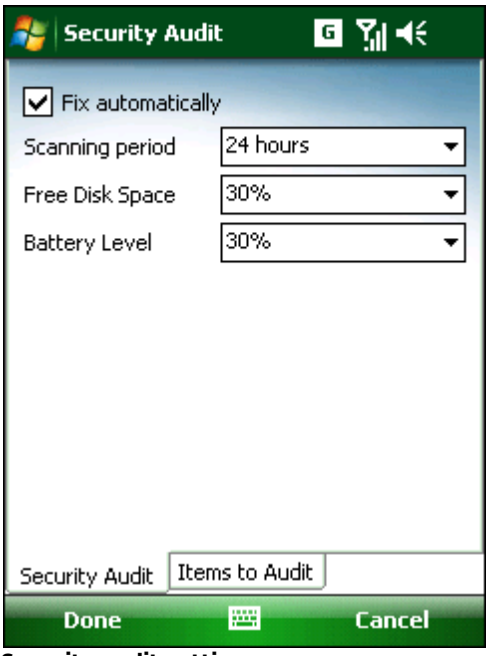
Running Processes

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 and its memory usage), select the process and tap **Details.**

9.1 Settings

To modify Security Audit parameters, tap **Menu > Settings > Security Audit.**



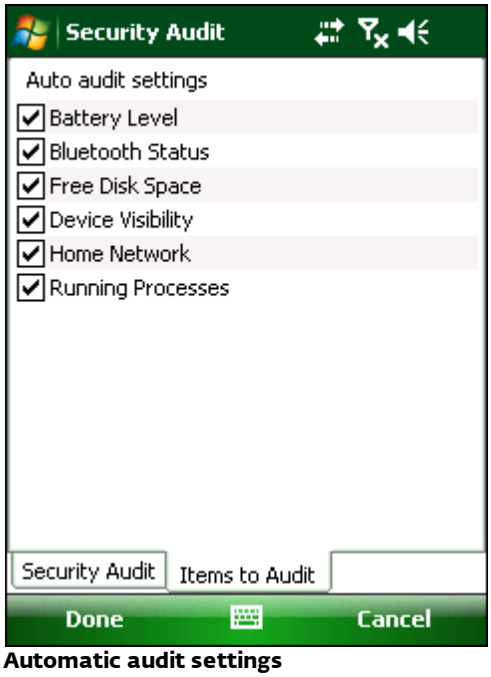
Security audit settings

If the **Fix automatically** box is checked, 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 **Items to Audit** tab, you can select the items to be checked during the automatic (scheduled) security audit.



Automatic audit settings

10. Spam filter

Spam filter 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 **Menu > View > Statistics** to see statistical information about received and blocked messages.

In the Spam filter settings (**Menu > Settings > Spam Filter**), the following filtering modes are available:

- **Block msg from contact list** – Enable this option to allow messages only from senders not included in your address book.
- **Block msg from unknown senders** – Enable this option to accept messages only from contacts in your address book.
- Select both **Block msg from contact list** and **Block msg from unknown senders** to automatically block all incoming messages.
- Deselect both **Block msg from contact list** and **Block msg from unknown senders** to disable the Spam filter. 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

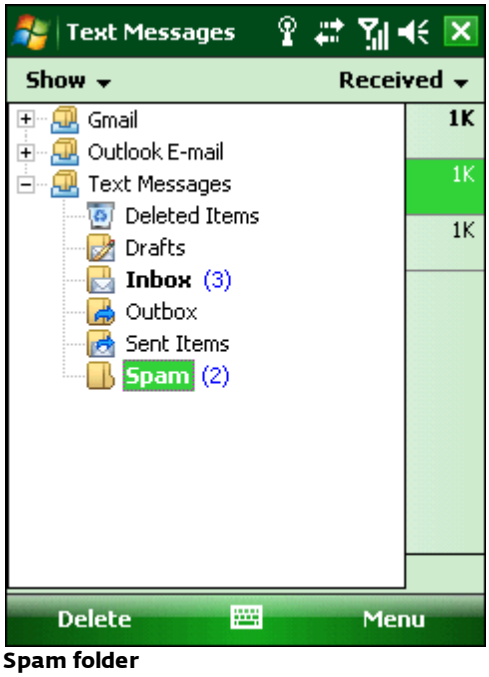
To add a new number to the Whitelist/Blacklist, select the tab for the list you wish to modify and tap **Options > Add.** To add a number from the contact list, tap **Options > Add contact.**

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 Spam filter settings. The folder is automatically created when the first spam message is received. To locate the **Spam** folder and review blocked messages, follow the steps below:

1. Open the program your device uses for messaging. For example, from the **Start** menu tap **Messaging**
2. Tap **Text Messages** (or **MMS** if you wish to locate the MMS Spam folder)
3. Tap **Menu > Go To > Folders ...** (for smartphones tap **Menu > Folders**)
4. Select the **Spam** folder.

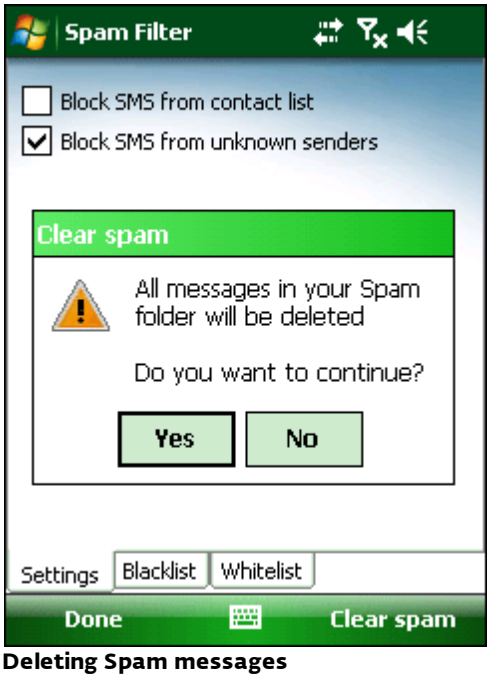


Spam folder

10.4 Deleting spam messages

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

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

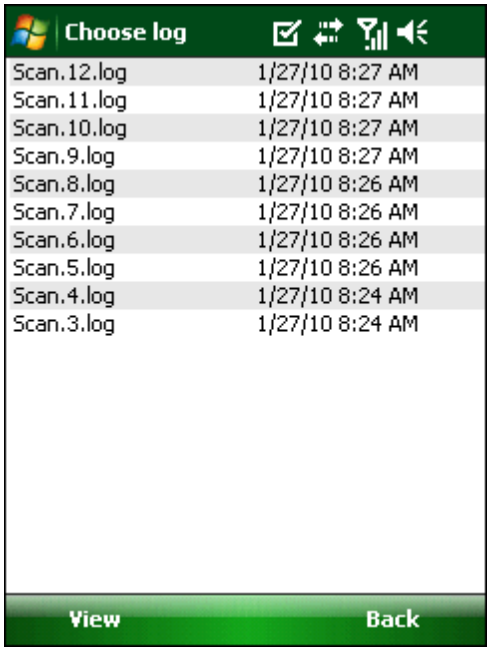


Deleting Spam messages

11. Viewing logs and statistics

The **Scan** log section (**Menu > 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.

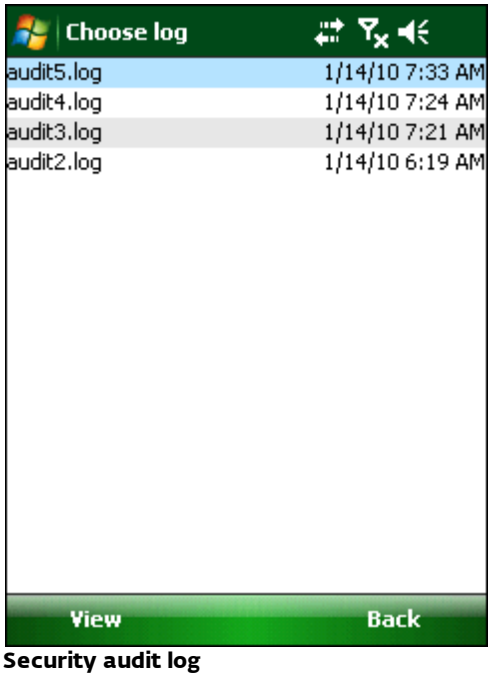
Logs contain:
- log file name (usually in the form *Scan.Number.log*)
- date and time of the event
- list of scanned files
- actions performed or errors encountered during the scan



Scan log

The **Security Audit** log section (**Menu > Logs > Security Audit**) stores all security audit results from both automatic (scheduled) audit and manually triggered audit.

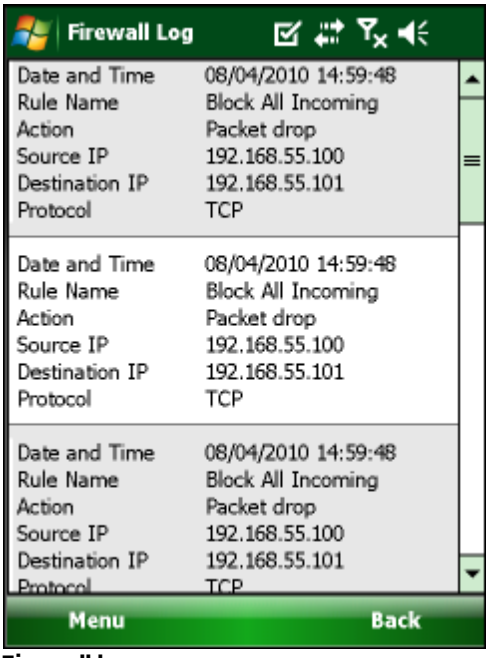
Logs contain:
- log file name (in the form *auditNumber.log*)
- date and time of audit
- detailed results



Security audit log

The **Firewall Log** (**Menu > Logs > Firewall**) contains the information about all firewall events. Log is updated after each communication performed through the firewall. New events appear on the top of the log.

Log contains:
- date and time of the event
- name of the rule used
- action performed (based on the rule settings)
- source IP address
- destination IP address
- protocol used

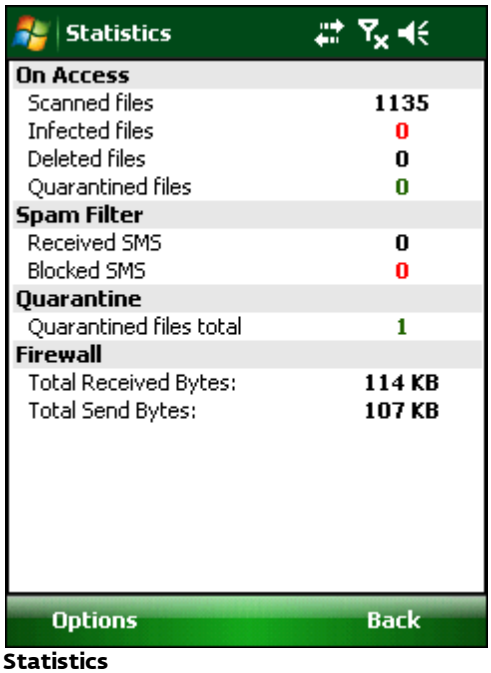


Firewall log

The **Statistics** screen (**Menu > View > Statistics**) displays a summary of:
- files scanned by the On-Access scanner
- received and blocked messages
- quarantined files
- received and sent data through firewall

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

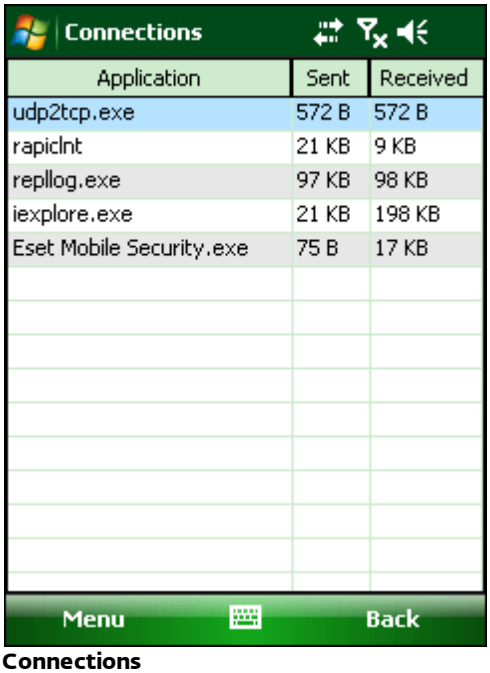
Reset counter.



Statistics

The **Connections** section (**Menu > View > Connections**) displays the applications used for sending and receiving data. Information includes:

- name of the process
- amount of data sent
- amount of data received



Connections

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 **Menu > Settings > Update** and you should see *updmobile.eset.com* in the **Internet 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.

12.4 Update file missing

If you are trying to update ESET Mobile Security using your computer, the virus signature database update file must be present in the program folder. See the Update using your computer 6 section for further details.

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