ESET
Mobile Antivirus

Installation Manual
and User Guide

we protect your digital worlds

ESET Mobile Antivirus

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

REV.20081119-003

contents

1. Installation of ESET Mobile Antivirus

1.1 Minimum system requirements

To install ESET Mobile Antivirus, your mobile device must meet the following minimum requirements:

ESET Mobile Antivirus	Recommended	Minimum
Processor	400 Mhz	200 Mhz
Memory	1 MB	
Operating System	Windows Mobile 5, 6.0, 6.1	

Most PDA and Smartphone mobile devices fulfill these requirements.

1.2 Installation

Save all open documents and exit all running applications before installing.

You can perform the installation from your computer via ActiveSync (or Windows Mobile Device Center in Windows Vista) or directly on the device.

1.2.1 Installation on the Device

To install ESET Mobile Antivirus directly on your device, download the .cab installation file by WiFi, Bluetooth file transfer, or email attachment (its purpose is similar to that of an .msi package on your PC).

After downloading, tap **Start > File Explorer** to locate the .cab file. Tap the .cab file to launch the installer.

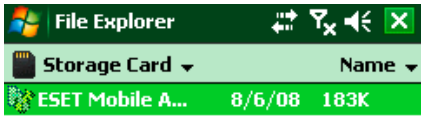

Figure 1-1 Installation package

After the installer runs, select **Device** as the installation location and tap **Install** to start the installation.

NOTE: The program must be installed on the device, not a memory card, in order to function properly.

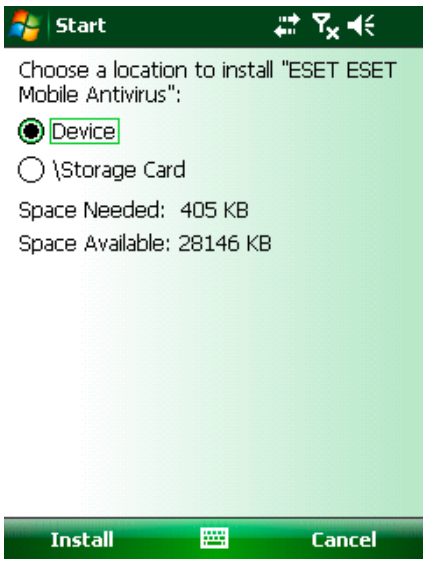

Figure 1-2 Select installation location

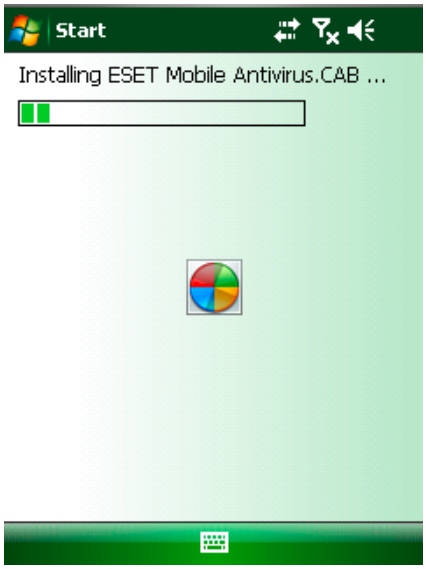

Figure 1-3 Installation progress

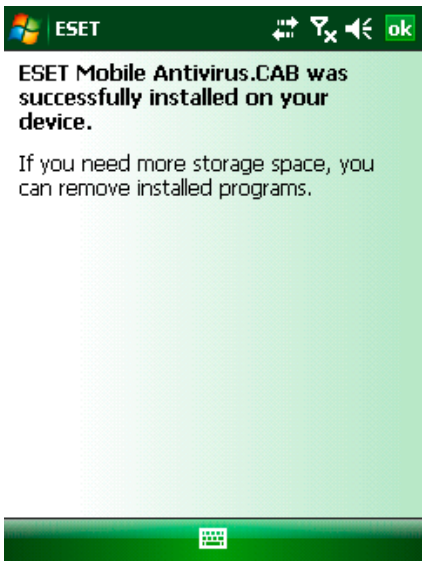

Figure 1-4 Installation is complete

The installation is complete when you see the message shown in Figure 1.4. Tap **ok** to complete the installation process.

After installation, you can modify the program's parameters. However, the ESET Mobile Antivirus default configuration provides the maximum level of protection against malicious programs.

1.2.2 Installation using your computer

To install ESET Mobile Antivirus using your computer (i.e., Active Sync in Windows XP or Windows Mobile Device Center in Windows Vista), download and then run the installation package (.exe file) on the computer to which your mobile device is connected.

Follow the instructions in the installation wizard.

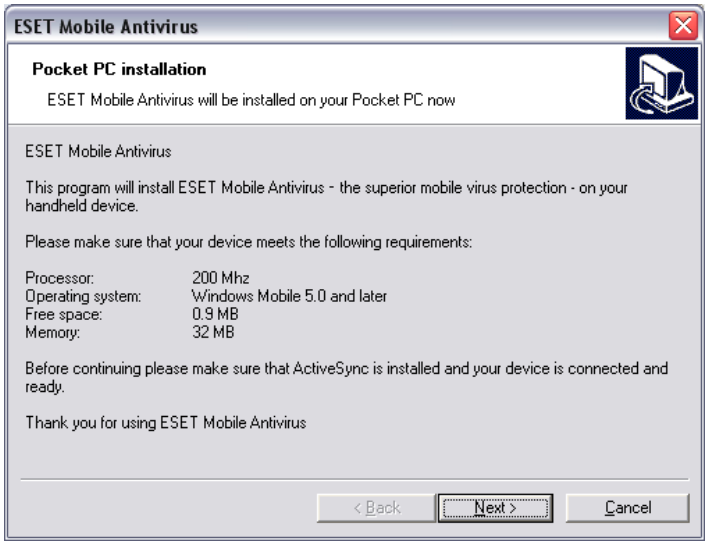

Figure 1-5 Launching the installer on a computer

Verify that your system meets the minimum requirements for ESET Mobile Antivirus (see section 1.1, "Minimum system requirements") and then click **Next** to proceed to the dialog window containing the program's End User License Agreement (EULA).

After accepting the EULA, click **Finish** to begin installing on your mobile device.

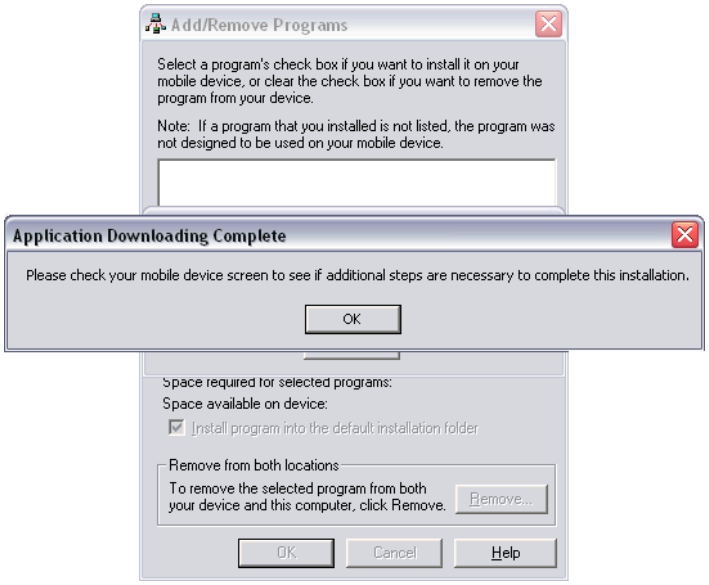

Figure 1-6 Installation on the computer is complete

After the installation package has been copied to your mobile device, click **OK** to exit the installer on your computer. To finish the installation, follow the steps described in section 1.2.1 using the .cab installation file.

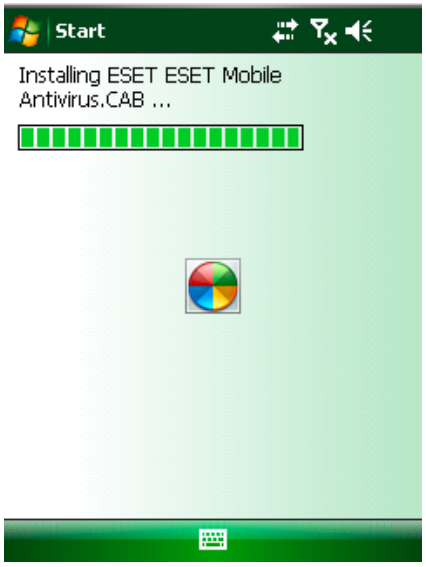

Figure 1-7 Installing the .cab file on the device

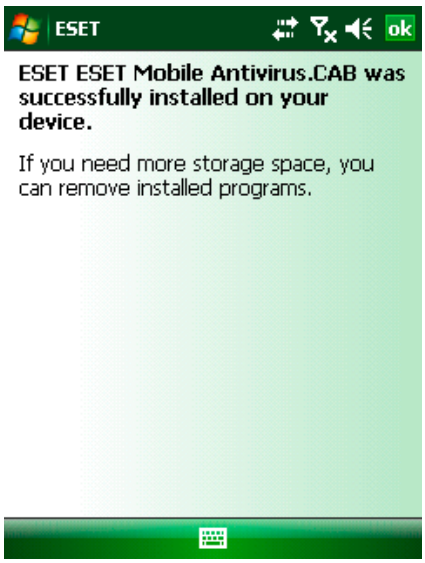

Figure 1-8 Installation is complete

When the installation is finished, the installer displays a message indicating that the program was successfully installed. Tap **ok** to exit the installation. Then, activate ESET Mobile Antivirus by following the steps in section 1.3 Product activation.

1.3 Product activation

After installation, ESET Mobile Antivirus must be activated in order to function.

There are two methods of activating ESET Mobile Antivirus, depending on whether your device is connected to the Internet or not.

1.3.1 Devices connected to the Internet

After you install the program and launch it for the first time, you will be prompted to enter your username, password (emailed to you upon purchase of the product) and email address. It is not required that this email address be the same as the one used to purchase ESET Mobile Antivirus.

After entering your username, password and email address, tap **Activate** to activate ESET Mobile Antivirus. An activation confirmation message will be sent to this email address.

Activation is also available through **ESET Mobile Antivirus** > **Menu** > **Activate**.

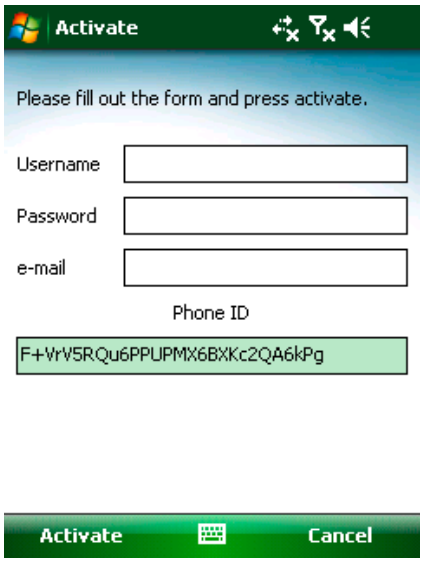

Figure.1-9 Program activation

Warning: During updates and when activating the product, a small amount of data must be downloaded from the Internet. These transfers are charged according to the pricelist of your mobile provider.

1.3.2 Devices not connected to the Internet

To activate ESET Mobile Antivirus on a device not connected to the Internet, you need to submit your Phone ID. This ID is shown at the bottom of the Activation window, which is displayed after you start the unactivated version of ESET Mobile Antivirus.

Copy the Phone ID, open your web browser and complete the activation form at http://www.eset.com/activate/mobile.php. The activation files will then be sent to the email address you entered in the activation form.

NOTE: The username and password needed to complete the activation form should already have been sent to the email address used to purchase ESET Mobile Antivirus.

Install the ESET Mobile Antivirus activation files to your device. Before installation, you must extract installation files from the delivered ZIP archive. The installation process depends on the file type used (.cab, .exe) – see section 1.3.2.1 below.

1.3.2.1 Program activation using EXE file (Active Sync)

1. Save the .exe email attachment to your hard drive
2. Connect your device to your PC using ActiveSync
3. Run the .exe file (your device should still be connected to your PC) to register ESET Mobile Antivirus
4. After activation is complete, an activation confirmation message will be displayed

1.3.2.2 Program activation using CAB file

1. Save the .cab email attachment to your hard drive
2. Connect your mobile device to your PC using ActiveSync
3. Copy the .cab file to the device
4. Run the .cab file from the mobile device
5. After activation is complete, an activation confirmation message will be displayed

1.4 Uninstalling

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

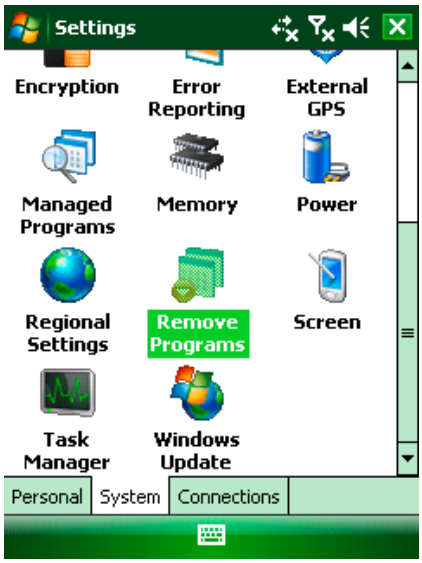

Figure 1-10 The Remove programs icon in the Settings menu

In the **Remove Programs** list, select **ESET Mobile Antivirus** and tap **Remove**. Tap **Yes** when prompted to confirm the uninstallation.

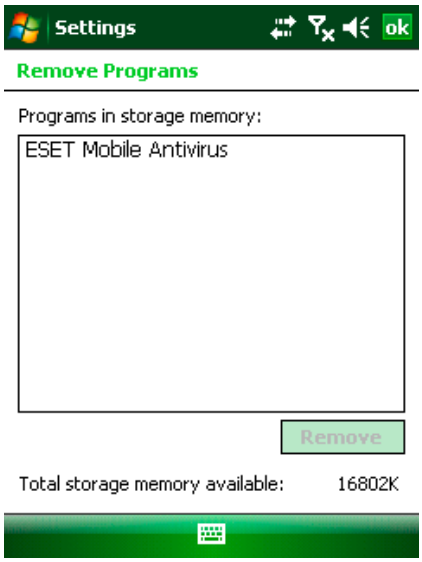

Figure 1-11 Select a program to be uninstalled

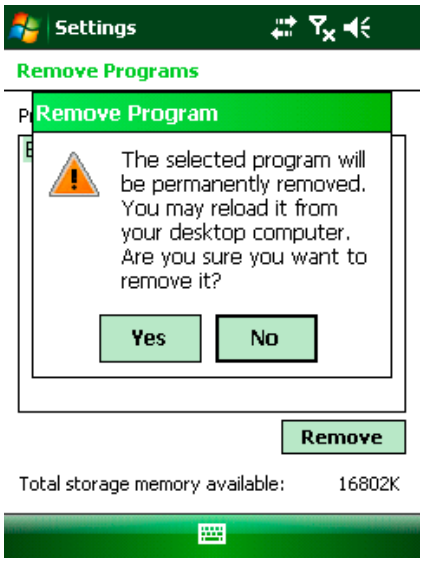

Figure 1-12 Confirm uninstallation

After the program has been removed, tap **ok** to close the **Remove Programs window**.

2. On-access scanner

Before we begin, note that the main ESET Mobile Antivirus window is the starting point for all instructions given in this manual. To access the main ESET Mobile Antivirus window, tap **Start > ESET Mobile Antivirus**.

The resident 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 the file, ensuring maximum protection. The On-access scanner is launched automatically at system startup.

2.1 Settings

In the **On-access settings** window (**Menu > Settings > On-access**), you can add or remove program features and also disable automatic program startup. The top part of the On-access settings window shows the number of scanned, infected and deleted files. The bottom section of the window contains the following options:

Enable On-access scan – If selected, ESET Mobile Antivirus runs resident in the background.

Heuristics – Select this option to apply heuristic scanning techniques.

Heuristics analyzes the code and searches for processes typical of virus behavior, in order to identify new malware that may not be detected by the virus signature database.

Run after restart – If selected, the On-access scanner will automatically initiate after restart.

Display scan in action status – Select this option to show information in the bottom right corner if scanning is in progress.

Show Shell Icon – Displays the ESET Mobile Antivirus icon on the main ESET Mobile window.

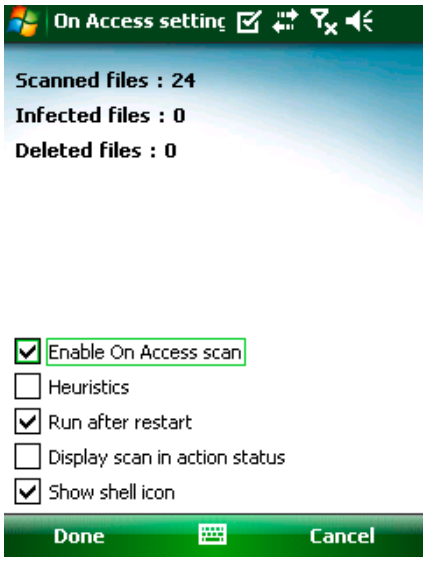

Figure 2-1 On-access scanner settings

2.2 Testing On-access Scanning

To verify that real-time protection is working properly, first select the **Display scan in action status** check box in the On-access settings window.

NOTE: Enabling the **Display scan in action status** option requires additional battery power, so we recommend leaving this option disabled (deselected) by default.

Next, open a file or initiate an activity (like playing a music file with the media player or taking a picture) A "Scanning..." message should appear briefly in the bottom right corner, as shown in Figure 2-2.

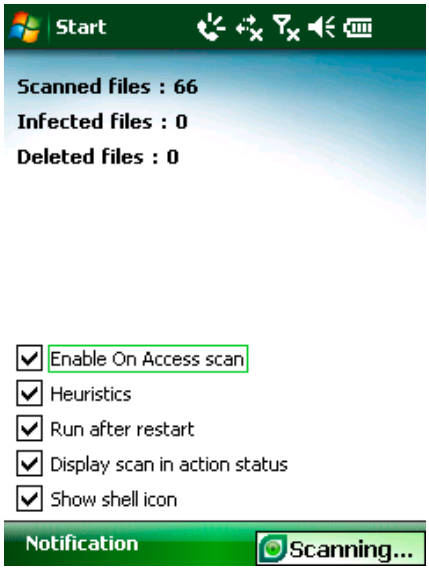

Figure 2-2 On-access Scanning

3. On-demand scanner

You can use the On-demand scanner to actively check your mobile device for the presence of infiltrations. By default, specific, predefined file types are scanned.

To run the On-demand scanner, tap **Scan** in the lower left corner of the main ESET mobile window.

Figure 3-1 An On-demand scan in progress

3.1 Running a Whole device scan

A Whole device scan checks memory, running processes, their dependent dynamic link libraries (DLL's), and files which are part of internal and removable storage.

NOTE: The memory scan is not performed by default. To activate it, tap **Menu** > **Settings** > **General** > **Memory Scan**

From the ESET Mobile window, tap **Scan > Whole device**. System memory is scanned first, including processes found running in it and their dependent DLL's. Files and folders are scanned next. The full path and file name of each file scanned will be briefly displayed.

Figure 3-2 Whole device scan

3.2 Scanning a folder

To scan a single folder on your device, tap **Start > ESET Mobile Antivirus**. From the lower left corner, tap **Scan > Folder**. Then, tap the folder you wish to scan and tap **Select** to begin scanning the chosen folder. If you enabled Memory Scan in **Menu** > **Settings** > **General** > **Memory Scan**, it is performed as well.

NOTE: To abort a running scan, tap **Menu > Stop Scan** from the bottom right.

Figure 3-3 Scanning a folder

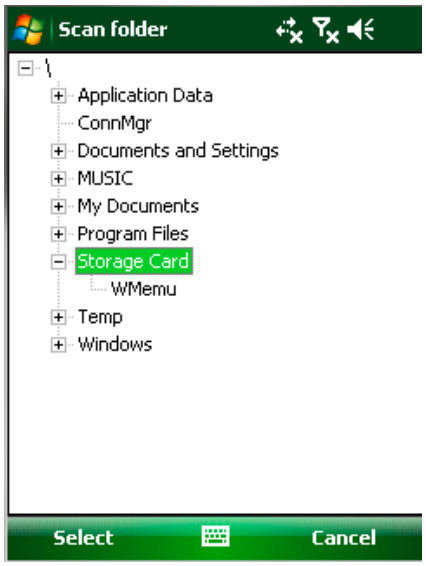

Figure 3-4 Choose the folder

3.3 Settings

To modify selected parameters of ESET Mobile Antivirus related to virus scanning, tap **Menu > Settings > General**.

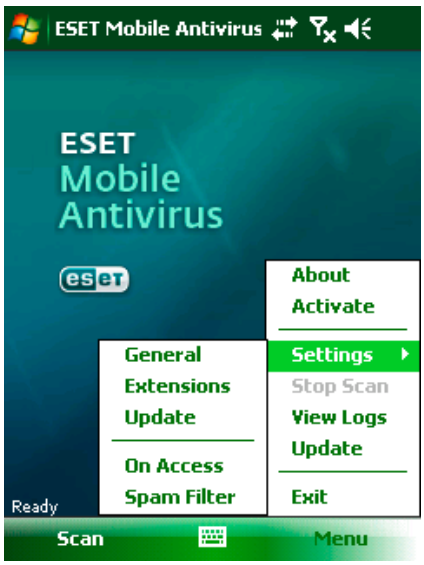

Figure 3-5 The Settings menu

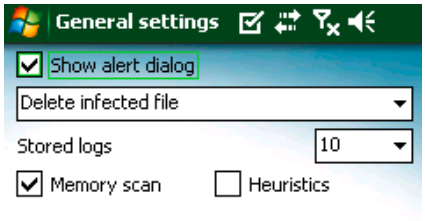

Figure 3-6 General settings

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

The drop-down menu below allows you to select an action to be automatically performed for infected files. The following options are available: **Delete infected file** and **Do nothing** (**not recommended**). If you enabled the **Show alert dialog** option, an alert window prompting you to confirm the predefined action (or enabling you to select other action) is displayed when an infiltration is found.

The **Stored logs** drop-down menu allows you to define the maximum number of logs to be stored.

If the **Heuristics** option is selected, ESET Mobile Antivirus uses heuristic scanning techniques. Heuristics is an algorithm-based detection method which analyzes the code and searches for typical virus behavior. Its main advantage is the ability to identify malicious software which may not be known by the current virus signature database.

Archive nesting allows you to specify the number of nested archives to be scanned.

Select the **Memory scan** check box to activate scanning of operating memory on your mobile device.

Select **Archive deletion** to automatically delete archive files which contain infected objects.

3.4 Scan objects setup

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

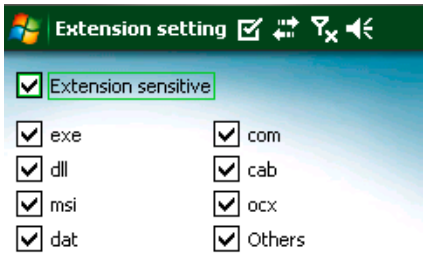

Figure 3-7 Advanced scan parameter setup

The **Extension setting** window will be displayed (Figure 3-7), showing the most common file types that are exposed to risk of infiltration. Select file types you wish to be scanned. To exclude an extension from scanning, deselect its check box.

To scan all files, deselect the **Extension sensitive** check box.

4. Virus found

If a virus is found, ESET Mobile Antivirus will prompt you to take an action. We recommend you select **Delete infected file**. If you select the other option – **Do nothing** – no action will be performed and the infected file will remain on your mobile device.

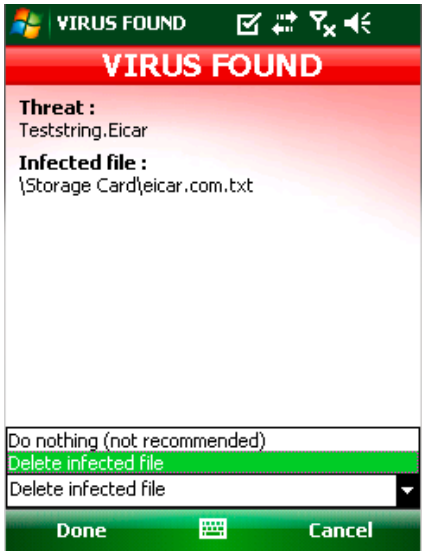

Figure 4-1 Action if a virus is found

Figure 4-2 Virus found

When a virus is detected, ESET Mobile Antivirus also displays the **Show alert dialog** check box. Deselect this option to prevent alert windows from displaying in the future. All actions will be performed automatically.

NOTE: When an infiltration is detected in an archive, the **Delete archive** option is available in the alert window. Select this option along with the **Delete infected files** option to delete all infected archive files.

5. Spam filter

The Spam filter serves to block unsolicited SMS messages which are sent to your mobile device.

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

5.1 Settings

At the top of the Spam Filter window (**Menu > Settings > Spam Filter**) you can see statistical information about the number of received and blocked messages.

In the Spam filter settings at the bottom, the following filter modes are available:

Block SMS from contact list – Enable this option to allow SMS messages only from senders that are not in your address book. The Whitelist and Blacklist entries override this option.

Block SMS messages from unknown sender – Enable this option to accept messages only from contacts in your address book. The Whitelist and Blacklist entries override this option.

Select both **Block SMS from contact list** and **Block SMS from unknown senders** to automatically block all incoming SMS messages. The Whitelist and Blacklist entries override this option (see section 5.2, "Whitelist/Blacklist").

Do not block messages – Deselect both options to disable the Spam filter. All incoming messages will be accepted. The Whitelist and Blacklist entries override this option (see section 5.2, "Whitelist/Blacklist").

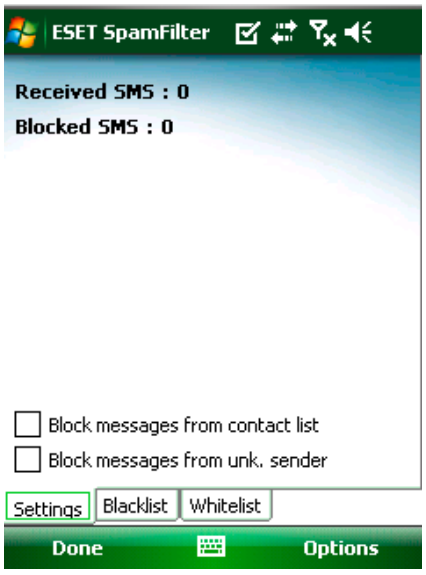

Figure 5-1 Spam filter

5.2 White / Black list

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

Figure 5-2 Spam filter's Whitelist

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

Warning: Adding a number/contact to the Blacklist will automatically move messages sent from those users to the Spam folder!

To add a number or a contact to Whitelist/Blacklist, tap **Options**.

Figure 5-3 Spam filter's Blacklist

5.3 Locating blocked (Spam) messages

The Spam folder is used to store blocked messages which are routed to it, and is automatically created upon detection of the first spam message. To locate the Spam folder and review blocked messages, follow the steps below:

1. Begin by opening the program which your device uses for text messaging. For example, from the Start menu tap **Messaging**.

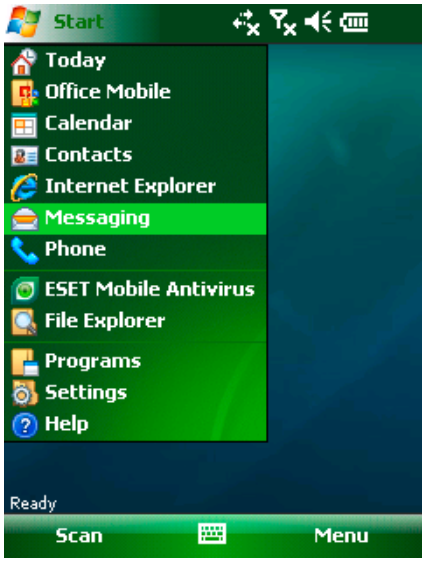

Figure 5-4 Tap Messaging

2. Tap **Messages** to open the list of received items.

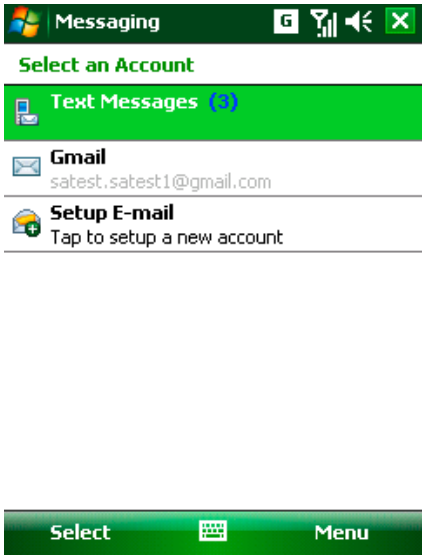

Figure 5-5 Tap Messages

NOTE: The system will likely point to the folder most recently visited. To switch to another folder, such

as the Spam folder, tap **Show** in the upper left (for Smartphones tap **Menu** > **Folders**).

3. Select the **Spam** folder.

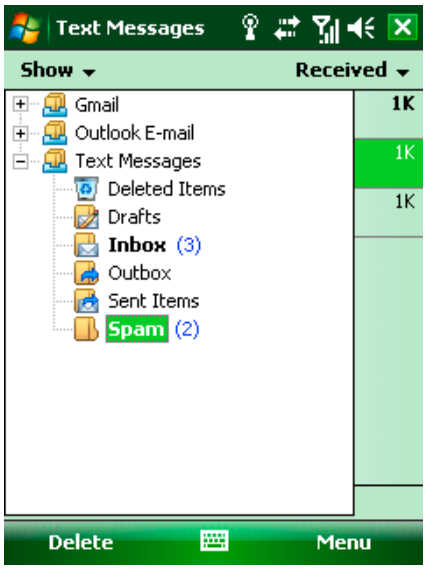

Figure 5-6 Spam folder

5.4 Deleting Spam Messages

To delete spam messages from your mobile device, follow the step by-step instructions below:

1. Tap **Menu >Settings > Spam Filter**.

2. Tap **Options** > **Clear spam**.

3. Tap **Yes** to confirm the deletion of all spam messages.

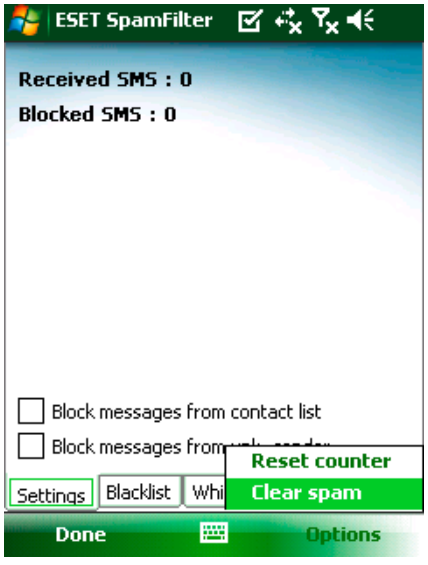

Figure 5-7 Deleting Spam Messages

By default, ESET Mobile Antivirus is installed with a predefined update task to ensure that the program is regularly updated. If necessary, you can perform updates manually.

After installation we recommend that you run the first update manually. To do so, tap **Menu** > and select **Update**.

Updating using your computer

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

1. Disable updating from the Internet in the **Miscellaneous settings** section (**Menu > Settings > Misc.**, deselect the **Internet update** option).

2. Download the file containing the most recent signatures to your PC.

3. Connect your device to your PC (Windows XP and earlier require that ActiveSync be installed. Windows Vista uses Windows Mobile Device Center).

4. Copy the virus signature update file (EsetAV_WM.upd) to the ESET Mobile Antivirus installation directory (e.g., Program Files\ESET\ESET Mobile Antivirus).

5. Tap **Menu > Update** – ESET Mobile Antivirus will check the update file. If the update file is not damaged, it will be installed.

6.1 Settings

To configure the virus signature update settings in ESET Mobile Antivirus, tap **Menu > Settings > Update**.

The **Internet update** check box toggles automatic updates. To set the time interval for the automatic update, use the **Auto update** drop-down menu. You can also specify the Internet server from which updates are downloaded , Usually, there is no reason to modify the predefined server u25.eset.com. In the **Login** and **Password** text fields enter the username and password you received after purchasing ESET Mobile Antivirus.

Figure 6-1 Update server/interval setup

Figure 6-2 Downloading updates

NOTE: Virus signature database updates are issued as needed, when a new threat occurs. This prevents unnecessary use of data bandwidth for your mobile device. Also note that while ESET provides virus signature database updates free of charge with your active product license, charges may result from your mobile service provider for data transfers. Please check with your mobile service provider. It is also possible to update the virus signature database manually using your computer. Please see chapter 6, "Update".

7. Viewing Logs

The **Choose log** section (**Menu > View Logs**) in ESET Mobile Antivirus stores all file scan results and scan status reports, along with information about locked and infected files.Logs are created when a scan is initiated, or when an infiltration is detected. All infected files are highlighted in red. At the end of each log entry you can find the reason why the file has been included in the log.

ESET Mobile Antivirus system logs contain the following information:

- Time – Date and time of the event
- Log name – Log file name.
  Usually in the form EsetAV_log_number.log
- Scanned files
- Actions performed or errors encountered during the scan

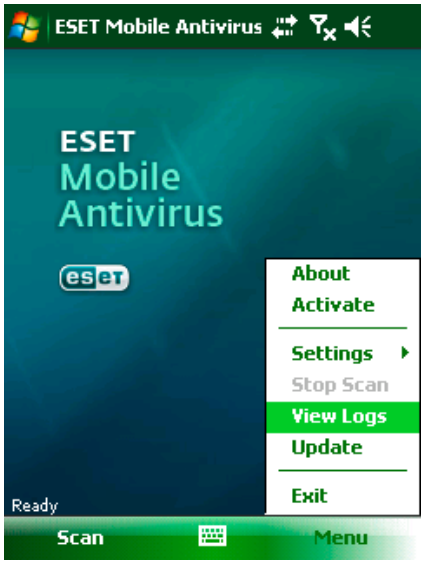

Figure 7-1 Opening scan log

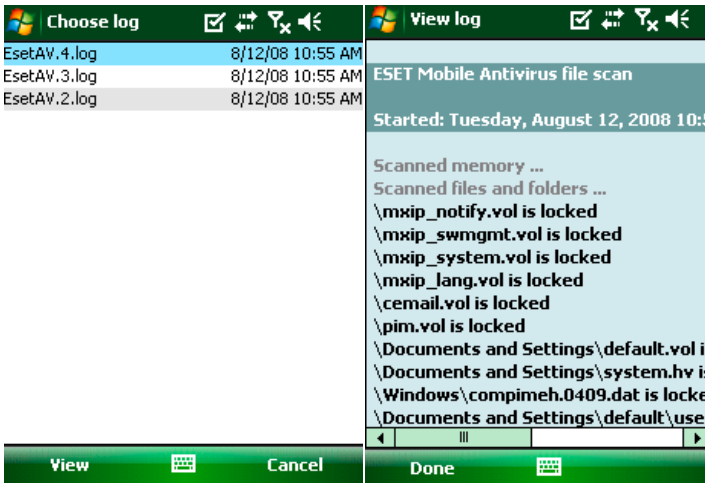

Figure 7-2 and Figure 7-3 Device scan logs

8. Troubleshooting

This section provides solutions to common questions about ESET Mobile Antivirus.

8.1 Connection to update server failed

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

Try the following:

1. **Check your Internet connection**

   Open your Internet browser to http://www.eset.com to verify that you are connected to the Internet

2. **Check if the program is using the correct update server.**

   To check the server address, tap **Menu > Settings > Misc.**; in the Internet server field, you should see **u25 eset.com**.

9. Technical support

For administrative assistance or technical support related to ESET Mobile Antivirus 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, here: http://www.eset.com/support/kb.php

The Knowledgebase contains an abundance of useful information on resolving the most common and current issues, with easy-to-use drill-down categories and an advanced keyword search.

To contact ESET's Customer Care Department use the support request form available here: http://www.eset.com/support/contact.php