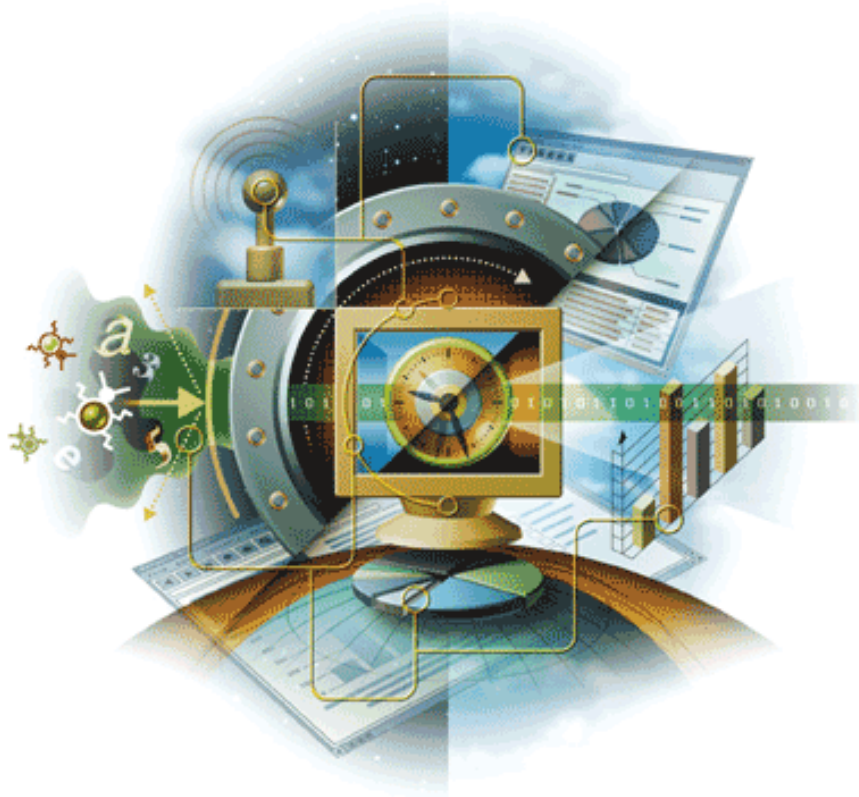


McAfee® VirusScan® Mobile


for Windows Mobile 5.0 SmartPhone and
Windows Mobile 6.0 Standard Edition
version 2.0.0



McAfee® System Protection

Industry-leading intrusion prevention solutions

McAfee®



McAfee[®] VirusScan[®] Mobile

for Windows Mobile 5.0 SmartPhone and
Windows Mobile 6.0 Standard Edition
version 2.0.0

McAfee[®]
System Protection

Industry-leading intrusion prevention solutions

McAfee[®]

COPYRIGHT

Copyright © 2007 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (AND IN KATAKANA), ACTIVESHIELD, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, EPOLICY ORCHESTRATOR, FIRST AID, FOUNDSTONE, GROUPSHIELD, GROUPSHIELD (AND IN KATAKANA), INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, MCAFEE, MCAFEE (AND IN KATAKANA), MCAFEE AND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NET TOOLS, NET TOOLS (AND IN KATAKANA), NETSCAN, NETSHIELD, NUTS & BOLTS, OIL CHANGE, PRIMESUPPORT, SPAMKILLER, THREATSCAN, TOTAL VIRUS DEFENSE, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (AND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (AND IN KATAKANA) are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. The color red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Attributions

This product includes or may include:

- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).
- Cryptographic software written by Eric A. Young and software written by Tim J. Hudson.
- Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that McAfee provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein.
- Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer.
- Software originally written by Robert Nordier, Copyright © 1996-7 Robert Nordier.
- Software written by Douglas W. Sauder.
- Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt.
- International Components for Unicode ("ICU") Copyright ©1995-2002 International Business Machines Corporation and others.
- Software developed by CrystalClear Software, Inc., Copyright ©2000 CrystalClear Software, Inc.
- FEAD® Optimizer® technology, Copyright Netopsystems AG, Berlin, Germany.
- Outside In® Viewer Technology ©1992-2001 Stellent Chicago, Inc. and/or Outside In® HTML Export, © 2001 Stellent Chicago, Inc.
- Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000.
- Software copyrighted by Expat maintainers.
- Software copyrighted by The Regents of the University of California, © 1996, 1989, 1998-2000.
- Software copyrighted by Gunnar Ritter.
- Software copyrighted by Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A., © 2003.
- Software copyrighted by Gisle Aas. © 1995-2003.
- Software copyrighted by Michael A. Chase, © 1999-2000.
- Software copyrighted by Neil Winton, ©1995-1996.
- Software copyrighted by RSA Data Security, Inc., © 1990-1992.
- Software copyrighted by Sean M. Burke, © 1999, 2000.
- Software copyrighted by Martinj Koster, © 1995.
- Software copyrighted by Brad Appleton, © 1996-1999.
- Software copyrighted by Michael G. Schwern, ©2001.
- Software copyrighted by Graham Barr, © 1998.
- Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000.
- Software copyrighted by Frodo Looijaard, © 1997.
- Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org.
- Software copyrighted by Beman Dawes, © 1994-1999, 2002.
- Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame.
- Software copyrighted by Simone Bordet & Marco Cravero, © 2002.
- Software copyrighted by Stephen Purcell, © 2001.
- Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>).
- Software copyrighted by International Business Machines Corporation and others, © 1995-2003.
- Software developed by the University of California, Berkeley and its contributors.
- Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).
- Software copyrighted by Kevlin Henney, © 2000-2002.
- Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002.
- Software copyrighted by David Abrahams, © 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation.
- Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000.
- Software copyrighted by Boost.org, © 1999-2002.
- Software copyrighted by Nicolai M. Josuttis, © 1999.
- Software copyrighted by Jeremy Siek, © 1999-2001.
- Software copyrighted by Daryle Walker, © 2001.
- Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002.
- Software copyrighted by Samuel Kremp, © 2001. See <http://www.boost.org> for updates, documentation, and revision history.
- Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002.
- Software copyrighted by Cadenza New Zealand Ltd., © 2000.
- Software copyrighted by Jens Maurer, ©2000, 2001.
- Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), ©1999, 2000.
- Software copyrighted by Ronald Garcia, © 2002.
- Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, ©1999-2001.
- Software copyrighted by Stephen Cleary (shammah@voyager.net), ©2000.
- Software copyrighted by Housemarque Oy <<http://www.housemarque.com>>, © 2001.
- Software copyrighted by Paul Moore, © 1999.
- Software copyrighted by Dr. John Maddock, © 1998-2002.
- Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999.
- Software copyrighted by Peter Dimov, © 2001, 2002.
- Software copyrighted by Jeremy Siek and John R. Bandela, © 2001.
- Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.
- Software copyrighted by Carnegie Mellon University © 1989, 1991, 1992.
- Software copyrighted by Cambridge Broadband Ltd., © 2001-2003.
- Software copyrighted by Sparta, Inc., © 2003-2004.
- Software copyrighted by Cisco, Inc. and Information Network Center of Beijing University of Posts and Telecommunications, © 2004.
- Software copyrighted by Simon Josefsson, © 2003.
- Software copyrighted by Thomas Jacob, © 2003-2004.
- Software copyrighted by Advanced Software Engineering Limited, © 2004.
- Software copyrighted by Todd C. Miller, © 1998.
- Software copyrighted by The Regents of the University of California, © 1990, 1993, with code derived from software contributed to Berkeley by Chris Torek.

Contents

1	Getting Started	6
	Features	6
	Installing VirusScan Mobile	7
	Uninstalling VirusScan Mobile	7
2	Using VirusScan Mobile	8
	Starting VirusScan Mobile	8
	Configuring VirusScan Mobile	9
	Enabling and disabling real-time scanning	9
	Configuring scan options	10
	Real-time scanning	10
	Message scanning	11
	Configuring VirusScan updates	12
	Configuring the quarantine area and log file sizes	12
	Scanning your device	13
	Using automatic scans	14
	Using manual scans	14
	Managing infected file warnings	15
	Updating VirusScan Mobile	15
	Automatically checking for updates	15
	Manually checking for updates	15
	Managing quarantined files	16
	Troubleshooting	18
	Viewing VirusScan Mobile program details	18
	Viewing the log	18
	Glossary	20
	Index	21

1

Getting Started

McAfee® VirusScan® Mobile 2.0.0 is an anti-virus solution for handheld devices, offering comprehensive, reliable, and up-to-date virus protection. Powered by McAfee scanning technology, VirusScan Mobile protects against threats from viruses, worms, Trojan horses, and Java applets before they can harm your device.

VirusScan Mobile provides:

Real-time scanning — Scan files when they are accessed by you or your device.

Automatic and manual scanning — Search for viruses and potentially harmful files on your device and removable storage cards.

Quarantine — Temporarily isolate infected and suspicious files in the quarantine folder until an appropriate action can be taken.

Features

McAfee VirusScan Mobile software provides the following features:

- **Complete protection**

VirusScan Mobile protects your mobile device from potentially harmful threats in SMS and MMS messages, and email messages and attachments.

- **Continuous protection**

VirusScan Mobile provides always-on protection, automatically scanning every file received by your mobile device.

- **Up-to-date protection**

Subscribers to the VirusScan Mobile security service get automatic updates to ensure that their devices are protected from the latest threats.

- **Small footprint**

Designed for the mobile world, VirusScan Mobile is small yet powerful, as well as easy to download and install.

- **Uninterrupted service**

Until it detects a threat, VirusScan Mobile runs silently on your device during mobile activities such as phone calls, data access, or web surfing.

Installing VirusScan Mobile

The VirusScan Mobile installation file is named in the following format:

VSM-SPTP-mmnn.CAB

where the “mmnn” part of the filename is numeric and indicates a version number.

The installation file can be obtained from McAfee by download or on removable storage media. The installation file can be run from either your device’s internal memory or removable storage media. If you downloaded the installation file, copy it to your device or a memory card. If you received the installation file on removable storage media, insert it into your device.

Copy the installation file from your computer to your SmartPhone (SP), then run it. You can use ActiveSync to transfer the .cab file from your computer to the SP. For instructions on doing this, see the ActiveSync documentation. Once you have transferred the .CAB file to your SP, follow the installation procedure below.

To install VirusScan Mobile:

- 1 Click **Start | File Manager**.
- 2 Go to the location (by default, the root directory) where you saved the .cab file.
- 3 Select the installation file to run it.
- 4 You must agree to the End User License Agreement (EULA) before the installation will proceed. Select **View EULA** to read the license agreement. Check **I Agree**. To start the installation, select **Done**. When the installation starts, a progress screen appears.

McAfee VirusScan appears in your Programs list. Also, a system tray icon indicates that the program is running.

Uninstalling VirusScan Mobile

To uninstall VirusScan Mobile:

- 1 From the Main menu, select **Start | Settings**.
- 2 Select **Remove Programs**.
- 3 From the displayed list, select McAfee VirusScan Mobile, then click **Menu | Remove**.
- 4 You are prompted to verify that you want the program permanently removed. Click **Yes** to continue or **No** to cancel.

If VirusScan Mobile uninstalls normally, no further action is required. However, under certain circumstances, the program may not uninstall normally. If this occurs, a screen displays informing you that you must restart the device. Click **Yes** to restart your device.

2

Using VirusScan Mobile

With VirusScan Mobile, you can scan files and messages, update your detection definitions, and schedule tasks to run automatically. You can also manage infected files in your quarantine area, and use the log file to get information about suspicious files detected by VirusScan Mobile and troubleshoot problems.

A user performs two main operations with VirusScan Mobile:

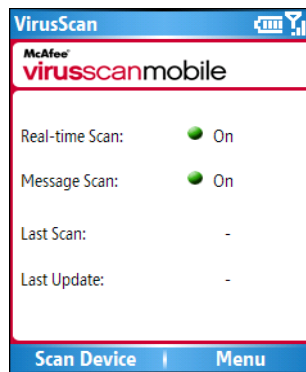
- Scanning messages when accessed or sent, and files at scheduled intervals, manually at any time, or when accessed.
- Updating VirusScan Mobile to use the latest detection definitions.

Both operations are accessed from the VirusScan Mobile main screen, and can be run manually or scheduled to run automatically. Configuration settings allow you to control all VirusScan Mobile features.

Starting VirusScan Mobile

To use VirusScan Mobile, click the device's **Start** menu, then select **McAfee VirusScan** from the list. The VirusScan Mobile main screen appears. By default, both real-time scanning and message scanning are enabled.

Figure 2-1 VirusScan Mobile main screen



The main screen shows which scanning methods are active, and when the last scan and last update occurred. To manually scan your device, select **Scan Device**. To configure and manage all VirusScan Mobile features, select **Menu**.

Configuring VirusScan Mobile

VirusScan Mobile has configuration options for:

- Enabling and disabling the real-time and message scanners.
- Configuring options for automatic real-time file and message scanning, including the action to take when an infected or suspicious file is detected.
- Configuring automatic and manual VirusScan product updates.
- Set the quarantine area size.
- Set the log file size.

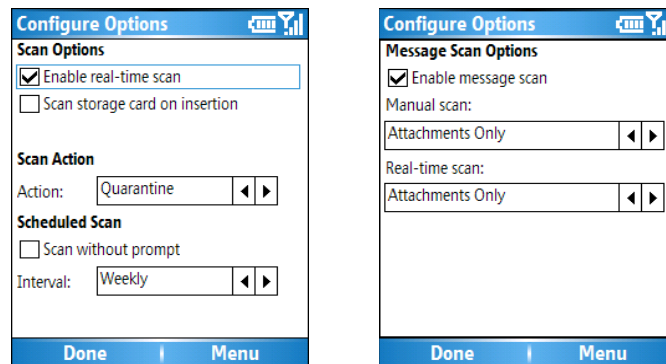
Enabling and disabling real-time scanning

Real-time scans check system resources for malicious content and viruses. These checks occur when files are added or changed, and when a message (such as an MMS or email) is sent or received. With the VirusScan Mobile real-time scanners enabled, files and messages are scanned before malicious content and viruses can harm your device.

To enable or disable the real-time scanners:

- 1 Click **Menu** and select **Configure Options**.
- 2 On the **Scan Options** page select or deselect the **Enable real-time scan** checkbox to enable or disable the real-time file scanner.
- 3 For message scanning, click **Menu** and select **Message Scan Options**. Select or deselect the **Message Scanning** checkbox to enable or disable the message scanner.

Figure 2-2 Accessing the real-time scanners



Configuring scan options

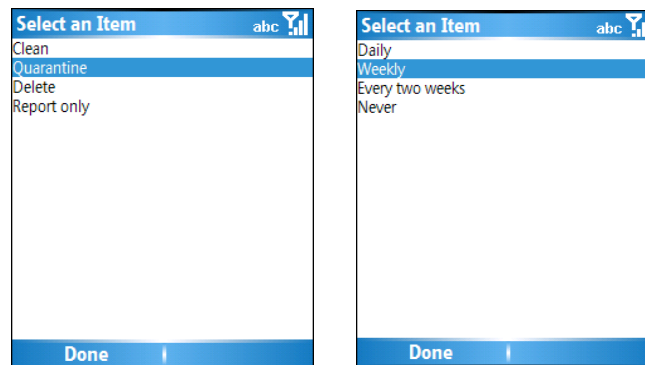
VirusScan Mobile has different configuration options for automatic real-time file scanning and message scanning.

Real-time scanning

To configure the real-time file scanning options:

- 1 From the main screen click **Menu**, select **Configure Options**.
- 2 On the **Scan Options** page click the appropriate checkbox to enable or disable the following options:
 - **Scan storage card on insertion** — when enabled, all files on a removable storage card are scanned immediately when the card is inserted in the device.
 - **Scan without prompt** — when enabled, you are not prompted before a scan is run. This option applies only to scheduled scans.
- 3 To set the **Scan Action**, and the interval for scheduled scans, highlight the field and press **Select**. A screen displays the options. You can also use the device's right and left arrows to scroll the selection list.

Figure 2-3 Scan action and scan interval options



The settings for these options are:

- **Scan Action** — Specifies the action to perform when an infected file is found. This setting applies to real-time scans and automatic scans. For information about setting the **Scan action** for manual scans, see [Using manual scans on page 14](#).

Clean — Repairs the infected file and device if possible.

Quarantine — Moves any infected files to the quarantine area. For more information, see [Managing quarantined files on page 16](#)

Delete — Removes the infected file.

Report only — Shows the file as infected, but does not take any action.

- **Scheduled Scan Interval** — Specifies how often to perform an automatic scan: **Daily**, **Weekly**, **Every two weeks**, or **Never**. This option is ignored when performing a manual scan.

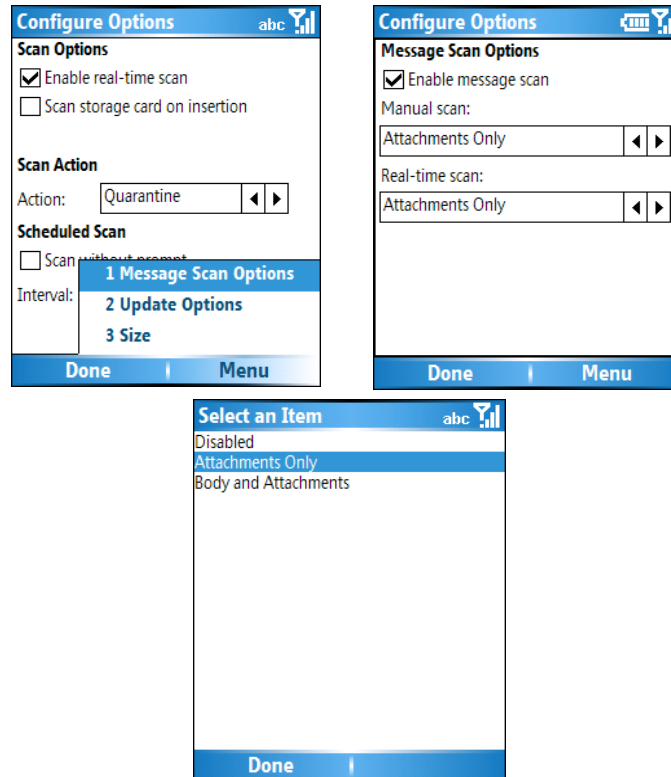
- 4 Click **Done** to save your settings.

Message scanning

To configure the message scanning options for automatic scans:

- 1 From the main screen click **Menu**, select **Configure Options**. From the Scan Options page, select **Menu** then select **Message Scan Options**.

Figure 2-4 Setting message scan options



- 2 To configure manual message scanning, highlight the **Manual Scan** field and press Select, or use the device's right and left arrows to scroll the selection list. The options are:

Disabled — Messages are not scanned during a manual scan even if Enable Message Scan is enabled.

Attachments Only — Only message attachments are scanned.

Body and Attachments — Both message attachments and the body of the message are scanned.

- 3 To configure automatic real-time message scanning, highlight the **Real-time Scan** field and press Select, or use the device's right and left arrows to scroll the selection list. The options are:

Disabled — Messages are not scanned during an automatic scan even if Enable Message Scan is enabled.

Attachments Only — Only message attachments are scanned.

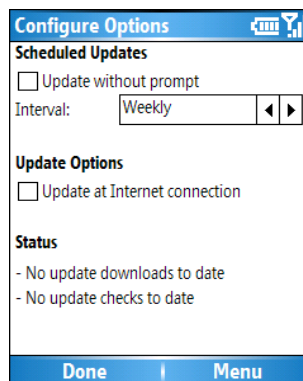
Body and Attachments — Both message attachments and the body of the message are scanned.

Configuring VirusScan updates

To configure update options:

- 1 From the main screen click **Menu**, select **Configure Options**. From the Scan Options page, select **Menu** then select **Update Options**.

Figure 2-5 Update options screen



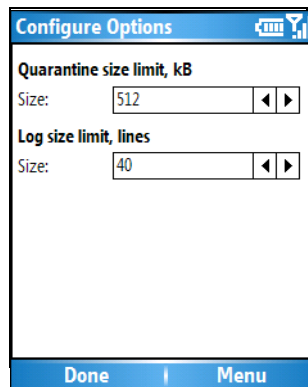
- 2 For scheduled updates, you have these options:
 - **Update without prompt** — when enabled, you are not prompted before an automatic update is run.
 - **Interval** — specifies how often to perform an automatic update. The settings are: **Daily**, **Weekly**, **Every two weeks**, **Monthly**, or **Never**. Highlight the **Interval** field and press Select, or use the device's right and left arrows to scroll the selection list.
- 3 General update options are:
 - **Update at Internet connection** — when enabled, an update is run when you connect to the Internet.
- 4 Click **Done** to save your settings.

Configuring the quarantine area and log file sizes

The quarantine area is where infected or suspicious files can be isolated when discovered during a scan. The log file records the activities performed by VirusScan Mobile, such as whether updates or scans have occurred, and whether suspicious files have been discovered during a scan. You can specify a size limit for each of these resources. To configure how much disk space to use for the quarantine area and the log file:

- 1 From the main screen click **Menu**, select **Configure Options**. From the Scan Options page, select **Menu** then select **Size**.

Figure 2-6 Configure quarantine area and log file sizes



- 2 The **Quarantine size limit** option displays the current size (in kilobytes) of the quarantine area. To change the value, use the device's right and left arrows to change the size in 32Kb increments.



If the quarantine area size limit is reached, the oldest files are removed to make room for new files being added.

- 3 The **Log size limit** option displays the current size of the log file in number of lines. To change the value (in increments of 10 lines), use the device's right and left arrows to scroll the selection list.
- 4 Click **Done** to save your settings.

Scanning your device

When the scanners are enabled, VirusScan Mobile performs real-time scanning, which automatically checks files and messages when they are accessed by you or your device. These scanners function as follows:

- **Real-time scanner** — Scans for malicious content when files are added or changed, or any system call is made.
- **Message scanner** — Scans for malicious content in SMS, MMS, and email messages and attachments when they are received or sent.

The real-time scanning functions automatically check any file that is accessed and any message sent or received. Automatic (scheduled) scans check your device's internal and external storage media at regular intervals. Manual scans check both internal and external storage media at any time.

When VirusScan Mobile finds an infected file, you can clean, quarantine, delete the file, or have VirusScan Mobile just report that it found an infected file. If VirusScan Mobile cannot clean the file, it can be quarantined or deleted. For more information, see [Managing quarantined files on page 16](#).

Scanning can be:

- Real-time — Occurs if the scanners are enabled (see [Enabling and disabling real-time scanning on page 9](#)).
- Scheduled — Occurs if the scanners are enabled, and the **Scheduled scan interval** setting is any value other than **Never**.
- User-initiated through a manual scan — Occurs if the scanners are enabled, and you click **Scan Device** on the VirusScan Mobile main screen.

Using automatic scans

Automatic scans thoroughly check your device's internal and external storage media for viruses and potentially harmful files at specified intervals. Scans automatically occur based on the **Interval** setting for scheduled scans (see [Configuring scan options on page 10](#)). If the **Interval** setting is **Never**, VirusScan Mobile does not perform automatic scans.

Using manual scans

A manual scan is one you initiate, and can run at any time. Manual scans are useful for checking content on internal and removable storage media before transferring files from your device to a computer.

To manually scan your device for viruses and potentially harmful files:

- 1 On the main screen, click **Scan Device**.
- 2 For the **Scan action** option, select which action to take if an infected file is found. The options are:
 - Clean** — Repairs the infected file and device if possible. If VirusScan Mobile cannot repair the file, an infected file warning appears (see [Managing infected file warnings on page 15](#)).
 - Quarantine** — Moves each infected file to the quarantine area.
 - Delete** — Removes the infected file.
 - Report only** — Shows the file as infected, but does not take any action.
- 3 Select **Scan Now** to start the scan. During scanning, the following is displayed:
 - Number of files scanned
 - Infected files detected
 - Name of the currently scanned file.

You can cancel the scan at any time by selecting **Cancel**. When the scan completes, a summary appears.
- 4 If the **Scan action** was set to **Quarantine** or **Report only**, click **Details** to view any infected files.
- 5 Click the infected file in the list to get more information about the file.

For information about handling infected or suspicious files, see [Managing infected file warnings on page 15](#) and [Managing quarantined files on page 16](#).

Managing infected file warnings

When VirusScan Mobile performs a scan, several situations can cause an infected file warning. This warning appears on the Scan Device screen when an infected file is found during a real-time scan, scheduled scan, or manual scan and when:

- The **Scan action** is set to **Clean, Quarantine, or Delete** and VirusScan Mobile cannot perform the appropriate action on the file.
- The **Scan action** is set to **Report only**.

To view information about infected or suspicious files detected, click **Details** when the warning is displayed, or on the Scan Device screen. The Scan Results screen displays any infected or suspicious files detected during the scan. Select a file from the list and click **Menu**. You can now clean, quarantine, or delete the file.

If you quarantine the file, it is moved to the quarantine area. For information about handling files in the quarantine area, see [Managing quarantined files on page 16](#).

Updating VirusScan Mobile

Updating VirusScan Mobile should be performed regularly to ensure that you always have the latest detection definitions. VirusScan Mobile can automatically check for updates at scheduled intervals, or you can manually check for updates at any time.



You must be connected to the Internet for VirusScan to check for available updates. If no direct connection is configured, you can connect through ActiveSync using your computer's Internet connection.

Automatically checking for updates

Automatic updates ensure that your device always has the latest virus protection. McAfee recommends that you check for detection definition updates often. Updates are checked for automatically based on the **Scheduled update interval** setting (see [Configuring VirusScan updates on page 12](#)).

If you do not want to automatically check for updates, set the **Scheduled update interval** to **Never**.

Manually checking for updates

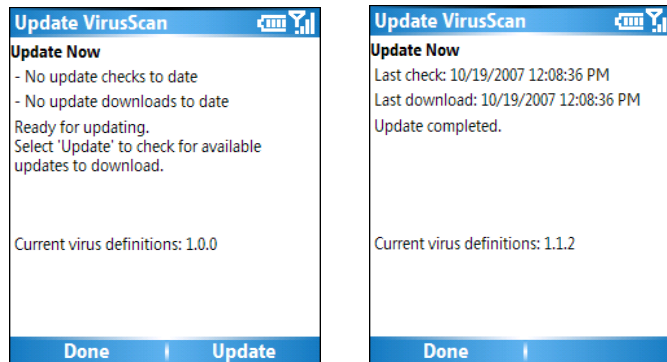
You can manually update your detection definitions at any time to ensure that your device has the latest virus protection.

To manually check for updates:

- 1 On the main screen, click **Menu** then select **Update VirusScan**.

- 2 Select **Update** to begin the update or **Done** to return to the main screen. If you want to cancel the update while it is occurring, click **Cancel**.

Figure 2-7 Updating VirusScan Mobile



If no updates are available, you are informed that your services are up-to-date. If **Scan after manual update** is enabled and **Scan without prompt** is disabled, you are prompted whether you want to scan your device when the update completes.

After the update is installed, the new signature version of the detection definitions is displayed, along with the previous version, the date and time of the last check, and the date and time of the last download. Click **Done** to return to the main screen.

Managing quarantined files

The Quarantine feature temporarily isolates infected and suspicious files in a quarantine area until an appropriate action can be taken. If cleaned, a quarantined file can be restored to its original location.

Items are added to the quarantine area when an infected file is found and:

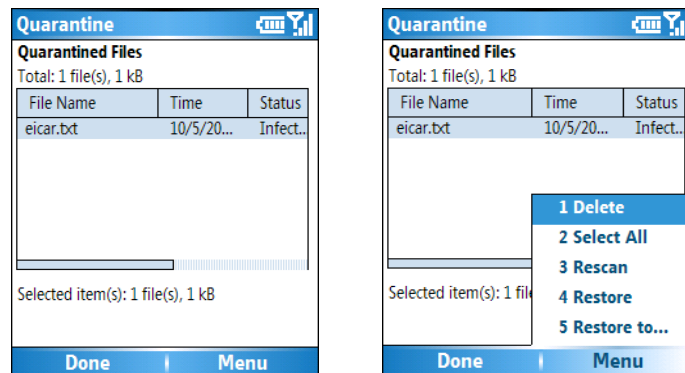
- the **Scan Action** is set to **Quarantine**.
- the **Scan Action** is set to **Report only** and you manually add a file from the Scan Results screen (see [Managing infected file warnings on page 15](#)).

To manage quarantined files:

- 1 From the main screen, click **Menu** and select **Quarantine**. The quarantine area displays a list of the quarantined files.
- 2 Select a file in the quarantine area to view more details about it.

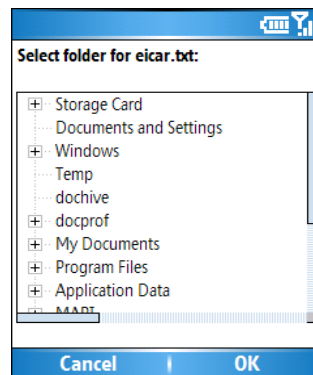
- 3 To select an action to perform on the quarantined file, click **Menu**. The options are:
- Select All** — Selects all files in the quarantine area.
 - Delete** — Removes the infected file from the device.
 - Rescan** — Scans the file again.
 - Restore** — Moves the file to its original location.
 - Restore To...** — Moves the file to a location you select on internal or external storage.

Figure 2-8 Viewing and taking action on quarantined files



- 4 If you chose **Restore to...**, the **Save As** screen appears where you can designate where to move the file. Select the location and select **OK** to restore the file, or **Cancel** to return to the Quarantined Files screen.

Figure 2-9 Restore To action on a quarantined file



- 5 Click **Done** when you are finished with the quarantined files.

To configure how much disk space to use for the quarantine area, see [Configuring the quarantine area and log file sizes on page 12](#).

Troubleshooting

To help with troubleshooting, you can view program details and the event log. In some situations, you might need to uninstall VirusScan Mobile as part of a troubleshooting strategy (see [Uninstalling VirusScan Mobile on page 7](#)).

Viewing VirusScan Mobile program details

You can view VirusScan Mobile program information from the **About** screen.

From the main screen, click **Menu**, then select **About**.

The **About** screen is updated after a successful update with:

- The build number.
- The detection definitions version.
- The date of last update.
- McAfee copyright information.

Figure 2-10 VirusScan Mobile About screen



Viewing the log

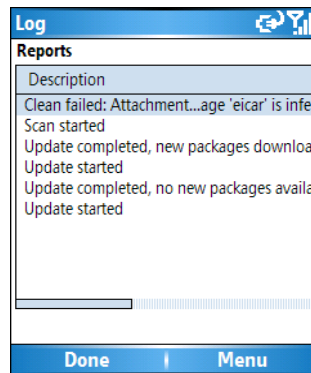
VirusScan Mobile records all activities it performs and information about detected viruses or suspicious content. It also can be useful in troubleshooting problems.

- 1** To view the log, click **Menu** from the main screen, then select **Log**.

The Log screen shows a list of log entries, with newer entries at the top. Use the horizontal scroll bar to view all information about the log entry.

- 2 Click **Done** to close the log file.

Figure 2-11 Viewing the log



To save the log (My Documents\VirusScan Mobile Report.txt), select **Menu | Save log** from the Log tab. To remove all entries from the log, select **Menu | Clear Log**.

To configure how much disk space to use for the log, see [Configuring the quarantine area and log file sizes on page 12](#).

Glossary

A

alert

A message or notification regarding computer activity such as detection.

automatic update

The automatic program in the McAfee software that updates that software program with the latest detection definition (DAT) files and scanning engine.

C

clean

An action taken by the scanner when it detects a *potentially unwanted program* or a *Trojan horse*. The cleaning action can include removing the potentially unwanted program from a file and restoring the file to usability; removing references to the potentially unwanted program from system files, and system .INI files; ending the process generated by the potentially unwanted program; deleting a macro that is threatening a file; deleting a file if it is a Trojan horse; renaming a file that cannot be cleaned.

L

log file

A record of the activities of the software. Log files record the actions taken during an installation or during the scanning or updating tasks.

Q

quarantine area

The location on a computer system that stores potentially unwanted programs until the system administrator can review them and decide on a course of action.

quarantine

Enforced isolation of a file or folder — for example, to isolate a threat — until action can be taken to clean or remove the item.

S

scan

A single scan event during which files are examined to determine if a potentially unwanted program or other potentially unwanted code is present.

U

updating

The process of installing detection definition file (DAT) updates.

Index

A

- About screen [18](#)
- automatic scanning [6, 14](#)
 - configuring [10](#)
 - message scanning options [11](#)
- automatic updates [6, 15](#)

B

- Bluetooth connections [6, 13](#)

C

- configuring
 - automatic scanning [10](#)
 - log file [12](#)
 - quarantine area [12](#)
 - updates [12](#)
 - VirusScan Mobile features [9](#)

D

- definition of terms (*See glossary*)
- Details screen, for infected files [14](#)
- disabling real-time scanning [9](#)

E

- email messages and attachments [6, 13](#)
- enabling real-time scanning [9](#)

F

- features
 - VirusScan Mobile [6](#)

G

- glossary [20](#)

I

- infected file warning [15](#)
- infected files
 - details about [15](#)
 - details screen [14](#)
 - setting the scan action [10, 14](#)
- installing VirusScan Mobile [7](#)

L

- log file
 - configuring [12](#)
 - size limit setting [13](#)
 - viewing [18](#)

M

- manual scanning [14](#)
 - infected file scan action
 - Clean [14](#)
 - Delete [14](#)
 - Quarantine [14](#)
 - Report only [14](#)
- manually updating VirusScan Mobile [15](#)
- message scanner [13](#)
- message scanning options [11](#)
- MMS messages [6, 13](#)

Q

- quarantine area
 - configuring [12](#)
 - size limit setting [13](#)
- quarantined files
 - deleting [17](#)
 - managing [16](#)
 - rescanning [17](#)
 - restoring [17](#)

R

- real-time scanner [13](#)
- real-time scanning
 - enabling and disabling [9](#)

S

- Scan Action setting
 - Clean [14](#)
 - Delete [14](#)
 - Quarantine [14](#)
 - Report only [14](#)
- Scan Device summary screen [14](#)
- Scan Results screen [15](#)
- scanning
 - automatically [14](#)
 - configuring [10](#)
 - email messages and attachments [6, 13](#)
 - files and messages [13](#)
 - manually [14](#)
 - scanning options
 - Scan action [10](#)
 - Scheduled scan interval [10](#)

- scanning, real-time
 - enabling and disabling [9](#)
- scheduled scanning [14](#)
- SMS messages [13](#)
- starting VirusScan Mobile [8](#)

T

- troubleshooting [18](#)

U

- uninstalling VirusScan Mobile [7](#)
- updating VirusScan Mobile [15](#)
 - automatically [6, 15](#)
 - configuring [12](#)
 - manually [15](#)

V

- viewing
 - log file [18](#)
 - VirusScan Mobile program details [18](#)
- virus warning
 - managing [15](#)
- viruses
 - scanning automatically [14](#)
 - scanning manually [14](#)
- VirusScan Mobile
 - configuring [9](#)
 - configuring updates [12](#)
 - footprint [6](#)
 - installing [7](#)
 - main screen [8](#)
 - starting [8](#)
 - troubleshooting [18](#)
 - uninstalling [7](#)
 - uninterrupted service [7](#)
 - updating [15](#)
 - updating automatically [15](#)
 - updating manually [15](#)
 - viewing program details [18](#)
- VirusScan Mobile features [6](#)
- VirusScan Mobile scanners
 - message [13](#)
 - real-time [13](#)

Copyright © 2007 McAfee, Inc. All Rights Reserved.

McAfee[®]

mcafee.com