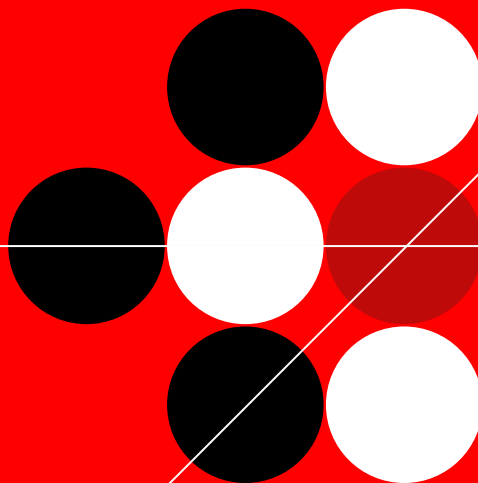


TREND MICRO™ Mobile Security 3 for Symbian OS™/S60

3rd Edition

User's Guide



Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme file and the latest version of the User's Guide, which are available from the Trend Micro Web site at:

<http://www.trendmicro.com/download/>

Trend Micro, the Trend Micro t-ball logo, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2004–2007 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Release date: April, 2007

The User's Guide for Trend Micro Mobile Security introduces the main features of the software and installation instructions. Trend Micro recommends reading it before installing or using the software.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. You can also evaluate this document at the following Web site:

<http://www.trendmicro.com/download/documentation/rating.asp>

Contents

Chapter 1: Introducing Trend Micro Mobile Security

Mobile Security Overview	1-2
Understanding Mobile Threats	1-2
Protecting Your Handheld Device	1-3
Mobile Security Features	1-3
Antivirus scanning	1-4
Regular component updates	1-4
Firewall	1-4
SMS anti-spam	1-5
WAP Push protection	1-5
Event logs	1-6

Chapter 2: Installing Trend Micro Mobile Security

System Requirements	2-2
Handheld device	2-2
Host computer	2-3
Before Installing	2-3
Getting the latest version	2-3
Obtaining a license	2-4

Installation	2-4
PC Suite installation	2-4
Bluetooth installation	2-5
Registration	2-6
Uninstallation	2-7

Chapter 3: Getting Started with Trend Micro Mobile Security

Updating Antivirus Components	3-2
Scanning for Viruses	3-3
Understanding the Interface	3-3
Main screen	3-4
Menu items	3-5
Reviewing Default Protection Settings	3-6

Chapter 4: Updating Antivirus Components

Connecting to ActiveUpdate Servers	4-2
Updating Program Components	4-3
Scheduled updates	4-3
Manual updates	4-6

Chapter 5: Scanning for Viruses

Antivirus Scan Types	5-2
Manual Scan	5-2

Real-time Scan	5-3
Enabling real-time scan	5-3
Setting the action on detected files	5-4
Card Scan	5-4
Scan Results	5-5
Viewing scan results	5-5
Handling detected or unscannable files	5-6
Quarantined Files	5-7
Advanced Antivirus Settings	5-8
Scanning compressed files	5-8
Configuring scan settings for compressed files	5-9
Information on Mobile Viruses	5-10

Chapter 6: Using the Firewall

Understanding Firewalls	6-2
Understanding Mobile Security Firewall Filtering	6-2
Predefined protection levels	6-3
Firewall rules	6-4
Enabling the Firewall	6-6
Configuring the Firewall Protection Level	6-6
Advanced Firewall Settings	6-7
Creating firewall rules	6-7
Setting firewall rule list order	6-11

Deleting firewall rules	6-12
Enabling intrusion detection	6-13

Chapter 7: Filtering SMS Messages

SMS Anti-spam Filter Types	7-2
SMS Anti-spam Configuration	7-3
Enabling SMS anti-spam filtering	7-3
Adding senders to your anti-spam list	7-4
Editing information on senders in your anti-spam list	7-7
Deleting senders from your anti-spam list	7-7
Blocking SMS messages from unidentified senders	7-8
Disabling SMS anti-spam filtering	7-9
Handling Blocked SMS Messages	7-10

Chapter 8: Filtering WAP Push Messages

Understanding WAP Push Messages	8-2
Enabling WAP Push Protection	8-3
Enabling WAP Push Notification	8-3
Managing the WAP Push Trusted Senders List	8-4
Adding trusted WAP Push senders	8-4
Modifying information on trusted WAP Push senders	8-5
Deleting trusted WAP Push senders	8-6
Handling Blocked WAP Push Messages	8-7

Chapter 9: Viewing Event Logs

Event Log Types	9-2
Scan log	9-2
Task log	9-4
Firewall log	9-6
Spam log	9-8
WAP Push log	9-10
Viewing Logs	9-12
Deleting Logs	9-13

Chapter 10: Troubleshooting, FAQ, and Technical Support

Troubleshooting	10-2
Frequently Asked Questions (FAQ)	10-4
Technical Support	10-7
Contacting Technical Support	10-7
Using the Knowledge Base	10-8
Sending security risks to Trend Micro	10-9
About TrendLabs	10-10
About Trend Micro	10-11

Glossary

Index

Introducing Trend Micro Mobile Security

Mobile Security is a powerful security solution for your phone and other handheld devices. Read this chapter to understand how Mobile Security can protect your handheld device.

This chapter covers the following topics:

- *Mobile Security Overview* on page 1-2
- *Understanding Mobile Threats* on page 1-2
- *Protecting Your Handheld Device* on page 1-3
- *Mobile Security Features* on page 1-3

Mobile Security Overview

Mobile Security is a full-featured security solution for phones and other handheld devices. It incorporates Trend Micro antivirus technology that is tailored to defend against the latest mobile threats, including viruses and other malware.

Mobile Security also allows users to filter unwanted Short Message Service (SMS) messages and Wireless Application Protocol (WAP) Push messages, which can initiate the delivery of unwanted content and applications.

Trend Micro Mobile Security 3.0 adds a robust firewall that can filter network communication. Users can select between three predefined firewall protection levels and define their own network filtering rules.

Understanding Mobile Threats

With the standardization of platforms and their increasing connectivity, handheld devices are susceptible to more threats. The number of malware programs that run on mobile platforms is growing and more spam messages are sent through SMS. New sources of content, such as WAP and WAP Push, are also used to deliver unwanted material.

In addition to threats posed by malware, spam, and other undesirable content, handheld devices are now susceptible to hacking and denial of service (DoS) attacks. Handheld devices, many of which now have the same network connectivity traditionally associated only with larger computing devices such as laptops and desktops, are now targets for such attacks.

Protecting Your Handheld Device

Users who practice safe computing habits are less susceptible to losing important data to viruses or becoming victims of fraud. To protect yourself, observe the following safe practices when using your handheld device:

- Use an antivirus product on the device and computers you use to connect to the device.
- If you connect your device to a network or the Internet, run a firewall on your device.
- Be wary of unsolicited WAP Push messages that prompt you to accept and install content. When the sender is unfamiliar to you and if you did not request or give prior consent to receive such content, do not accept the content.
- Be wary of SMS messages that tell you that you have won something, especially if these messages instruct you to send money or disclose personal information.
- Do not install or run applications received through unsolicited Bluetooth messages. When in a public area, avoid leaving your Bluetooth radio on.

Mobile Security Features

Mobile Security offers the following features:

- *Antivirus scanning* on page 1-4
- *Regular component updates* on page 1-4
- *Firewall* on page 1-4

- *SMS anti-spam* on page 1-5
- *WAP Push protection* on page 1-5
- *Event logs* on page 1-6

Antivirus scanning

Mobile Security incorporates award-winning Trend Micro technology to detect viruses and other malware, spyware/grayware, and files that can take advantage of vulnerabilities in your handheld device. Mobile Security is specially designed to scan for mobile threats and allows you to quarantine or delete detected files.

Regular component updates

To protect against the most current threats, you can either update Mobile Security manually or set it to update automatically.

Firewall

Trend Micro Mobile Security 3.0 includes the Trend Micro firewall module, which several award-winning Trend Micro products incorporate. With the firewall, you can use predefined security levels to filter network traffic. You can also define your own filtering rules and filter network traffic from specific IP addresses and on specific ports. The intrusion detection system (IDS) allows you to

block attempts to continually send multiple packets to your device. Such attempts typically constitute a denial of service (DoS) attack and can render your device too busy to accept other connections.

SMS anti-spam

Handheld devices often receive unwanted messages or spam through SMS. To filter unwanted SMS messages into a spam folder, you can specify the phone numbers from which all SMS messages will be considered spam or you can specify a list of approved phone numbers and configure Mobile Security to filter all messages from senders that are not in the approved list. You can also filter unidentified SMS messages or messages without sender numbers to prevent anonymous spam from reaching your inbox.

WAP Push protection

WAP Push is a powerful method of delivering content to handheld devices automatically. To initiate the delivery of content, special messages called WAP Push messages are sent to users. These messages typically contain information about the content and serve as a method by which users can accept or refuse the content.

Malicious users have been known to send out inaccurate or uninformative WAP Push messages to trick users into accepting content that can include unwanted applications, system settings, and even viruses.

Mobile Security lets you use a list of trusted senders to filter WAP Push messages and prevent unwanted content from reaching your device.

Event logs

You can view event logs to see details on detected viruses, firewall filtering results, filtered spam and WAP Push messages, and the results of update and scan tasks.

Installing Trend Micro Mobile Security

Mobile Security installation is a simple process that requires some preparation. Read this chapter to understand how to prepare for and continue with the installation.

This chapter covers the following topics:

- *System Requirements* on page 2-2
- *Before Installing* on page 2-3
- *Installation* on page 2-4
- *Registration* on page 2-6
- *Uninstallation* on page 2-7

System Requirements

Before installing and using Mobile Security, ensure that your handheld device and the host computer to which you are connecting it meet the requirements below.

Handheld device

Ensure that your handheld device meets the following requirements:

- **Operating system**—S60 3rd edition platform for Symbian OS
- **Storage space**—1MB minimum free space
- **Memory**—2MB minimum free memory; 3MB recommended



You can install Mobile Security only to your device's internal storage space, not to a memory card.

Supported devices

Mobile Security has been tested to work on the following Nokia™ phone models: E50, E60, E61, E62, E70, N93, N91, N80, N73, N71, 3250, and 5500.

Host computer

You can install Mobile Security through a host computer. To do this, you need a Microsoft™ Windows™-based computer running a version of PC Suite that is compatible with your device.

Before Installing

Before you install Mobile Security on your handheld device, check whether you have the latest installer and have your Activation Code ready.

Getting the latest version

Ensure that you have the latest installer for Trend Micro Mobile Security 3.0. To access the latest version, visit the following sites:

- On your standard Web browser, visit:
<http://www.trendmicro.com/download/product.asp?productid=54>
- On your WAP browser, visit:
<http://www.trendmicro-europe.com/pda/download.php>

Obtaining a license

If you have a current, unexpired license for Trend Micro Mobile Security 2.0, you do not need to obtain a new license to use version 3.0.

To purchase a new license, visit:

<http://www.trendmicro.com/tmms/buy>

Installation

There are several ways to install Mobile Security. Most users will find the following methods practical:

- **PC Suite**—open the installation file on a host computer while it is connected to your device through PC Suite
- **Bluetooth**—open the setup program directly on your device after transferring it using Bluetooth

To begin installation, you need the installation file `MobileSecurity.sis`.

PC Suite installation

To install Mobile Security from a host computer, use PC Suite.

To install using PC Suite:

1. Copy the installation file `MobileSecurity.sis` to the host computer.
2. Connect your device to the host computer with PC Suite.

3. On the host computer, open the installation file. The PC Suite installer opens and prompts you to begin the installation.
4. Start the installation. A message appears to inform you to check your device for further instructions.
5. Click **OK** on the prompt.
6. Follow the instructions on your device to complete the installation.
7. Mobile Security will prompt you to restart your device. Restart your device to ensure that all product modules are loaded.

When the installation completes, Mobile Security is added to your device's **Applications** menu.

Bluetooth installation

Use Bluetooth to transfer the installation file to your device and install Mobile Security.

To install via Bluetooth:

1. Transfer the installation file, `MobileSecurity.sis`, to your device using a Bluetooth-enabled computer. Your device prompts you that you have received a file.
2. On the device, select **Show**. The **Install software** prompt appears.
3. Select **Yes**. Product details display.
4. Select **Continue**. The license agreement displays.
5. Carefully read the license agreement.

6. Click **OK** to continue installation. A prompt appears informing you that Mobile Security can only be installed in internal memory.
7. Select **OK**. The installer extracts the SIS file.
8. The installer describes how Mobile Security uses your device's features. Click **Continue**.

When the installation completes, Mobile Security is added to your **Applications** menu.



Mobile Security will require a restart to load the firewall or the WAP Push protection driver.

Registration

The first time you launch Mobile Security, the **Register** screen appears and prompts you to enter an Activation Code. You can provide the Activation Code to register the product or use the product with a trial license for thirty days. You can also open the **Register** screen from the main screen.

To register Mobile Security:

1. On the main screen select **Options > Register**. The registration screen opens.
2. Enter the Activation Code, then select **Options > Register**.



At expiration of your license, all update features will be disabled.

Uninstallation

To remove Mobile Security, use your device's application manager.

To uninstall directly on the device:

1. On the device, go to **Menu > Tools > Application manager**.
2. Scroll to **Mobile Security**.
3. Select **Options > Remove**.



Figure 2-1. Register screen

4. When prompted for confirmation, select **Yes**.
5. When Mobile Security prompts you to save settings, select either of the following:
 - **Yes** to save your current settings, including firewall rules and anti-spam lists, so you can use them when you reinstall Mobile Security.
 - **No** to delete your current settings.

Getting Started with Trend Micro Mobile Security

You can start using Mobile Security immediately after installation. Read this chapter to understand the basic tasks, the main screen and its menu, and the default product settings.

This chapter covers the following topics:

- *Updating Antivirus Components* on page 3-2
- *Scanning for Viruses* on page 3-3
- *Understanding the Interface* on page 3-3
- *Reviewing Default Protection Settings* on page 3-6

Updating Antivirus Components

To ensure that you have the latest protection against mobile viruses and other malware, update Mobile Security after installation.

To update Mobile Security:

1. Select **Options > Update**. Mobile Security prompts you to specify a connection access point.
2. Select a valid access point. Mobile Security connects to the Internet through the selected access point.
3. Mobile Security will prompt you if you need to restart the device. Restart the device when prompted.



For more information on updating the product, see [Updating Antivirus Components](#) on page 4-1.

Scanning for Viruses

To immediately check your device for viruses, select **Options > Scan** on the main screen. You can delete or quarantine detected and unscannable files.



For more information on Mobile Security antivirus capabilities, see [Scanning for Viruses](#) on page 5-1.

Understanding the Interface

Mobile Security has a simple interface that allows you to easily understand and access different product features. The main interface includes the following:

- Main screen
- Menu items

Main screen

Mobile Security opens with its main screen. The following actions are available on the main screen:

Interface Item	Action
1	Enable or disable the real-time scan
2	Select between predefined firewall protection levels or disable the firewall
3	Access product features and settings

TABLE 3-1. Main screen interface items



Figure 3-1. Main screen

Menu items

The main screen's **Options** menu lets you access all product features. The menu items and the actions they perform are:

Menu Item	Action
Scan	Scan your device for mobile viruses and other malware
Update	Check for updates
Settings	Configure product settings
Event Logs	View event logs
Quarantine List	Access quarantined files
Virus Definitions	View definitions of known mobile malware
Register	Register the product
About	View the About screen
Help	View the Help

TABLE 3-2. Menu items on the main screen

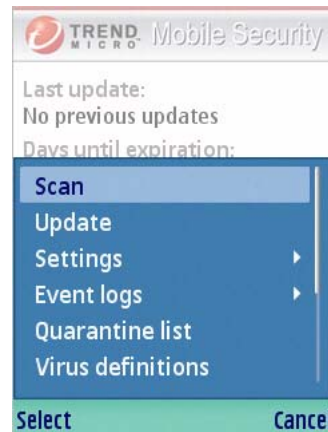


Figure 3-2. Main screen options

Reviewing Default Protection Settings

After installation, Mobile Security is ready to protect your device against mobile viruses and other threats. Review the default protection settings shown in Table 3-3 to assess whether you want to modify them.

Feature	Default Setting	Resulting Action
Real-time scan	Enabled	Product scans files that are being accessed.
Default action	Quarantine	Product encrypts and moves files detected by the real-time scanner.
SIS/ZIP scan level	3 (maximum)	Product extracts compressed files (ZIP/SIS) to up to three compression layers before scanning them for viruses. If a file is compressed in more than three layers, product considers the file unscannable.
Card scan	Disabled	Product does not scan memory cards automatically when inserted.
Connection alert	Enabled	Product displays a confirmation message before connecting to the Internet using GPRS, Wi-Fi, or IP passthrough.
Scheduled updates	Enabled	Product automatically checks for, downloads, and installs updates.

TABLE 3-3. Default protection settings

Feature	Default Setting	Resulting Action
Update frequency	8 hours	Product attempts to check for updates every time you connect your phone to the Internet if 8 hours has elapsed since the last update.
Force update after	30 days	Product runs an update after 30 days since the last successful download and installation of new components. It opens a wireless connection when necessary.
Firewall	Enabled	Product filters incoming and outgoing network traffic. See <i>Firewall rules</i> on page 6-4 for information on default firewall rules.
Intrusion detection system (IDS)	Enabled	Product protects against denial of services attacks.
Firewall protection level	Medium	Firewall allows all outgoing traffic and blocks all incoming traffic. Note that Mobile Security includes predefined firewall rules, which take precedence over the selected protection level.

TABLE 3-3. Default protection settings (continued)

Feature	Default Setting	Resulting Action
SMS anti-spam	Use blocked list	Product allows all SMS messages to reach the messaging inbox, except for messages from specified senders.
WAP Push protection	Disabled	Product does not filter WAP Push messages and allows all messages to reach the device.
Connection access point	Always ask	Product prompts you to select an access point every time it connects to the Internet.

TABLE 3-3. Default protection settings (continued)

Updating Antivirus Components

To stay protected against the latest mobile viruses and other malware, update the antivirus components regularly.

This chapter covers the following topics:

- *Connecting to ActiveUpdate Servers* on page 4-2
- *Updating Program Components* on page 4-3

Connecting to ActiveUpdate Servers

To update Mobile Security, you must connect to Trend Micro ActiveUpdate™ servers through the Internet. You can configure how Mobile Security connects to the Internet by specifying the access points.

To configure connection settings:

1. Select **Options > Settings > Advanced settings**. The **Advanced settings** screen opens.
2. Scroll to **Access point** and press the scroll key to select either of the following options:
 - **Use default**—select this option to specify an access point that will be used by Mobile Security automatically every time it connects to the Internet.
 - **Always ask**—select this option to set Mobile Security to prompt for the access point every time it connects to the Internet.



To define more access points, edit your device's connection settings. See your device's documentation for more information.



Figure 4-1. Connection settings screen

Updating Program Components

You can configure Mobile Security to update components automatically or you can update antivirus components manually. Mobile Security has three types of updates.

Type		Description
Manual		User-initiated; you can run these updates anytime.
Scheduled	Automatic	This update runs whenever you connect your phone to the Internet if the specified update interval since the last successful update check has elapsed.
	Forced	This update runs when the specified interval has elapsed since the last successful download and installation of new components. Forced updates will open the default wireless connection if your device is not connected to the Internet.

TABLE 4-1. Update types

Scheduled updates

Scheduled updates run at the intervals that you specify. To set these intervals, access the **Update settings** screen.

To configure the intervals between scheduled updates:

1. Select **Options > Settings > Update settings**. The **Update settings** screen opens
2. On the **Update settings** screen, ensure that **Scheduled updates** is enabled.
3. Scroll to **Update frequency** and press the scroll key to select your preferred interval. Mobile Security will attempt to check for updates whenever you connect your phone to the Internet if the specified interval has elapsed since the last successful update check.



Figure 4-2. Update settings screen

4. Select an interval for forced updates under **Force update after**. Mobile Security will open an Internet connection and check for updates when the specified interval has elapsed since the last successful download and installation of new components.
5. Select **Back**.



*Mobile Security may automatically open the default access point during forced updates. If you want Mobile Security to display a message before opening a wireless or IP passthrough connection, enable **Connection alert**.*



Figure 4-3. Wireless connection alert

Manual updates

To perform a manual update:

1. Select **Options > Update**. Mobile Security prompts you for the access point or automatically connects to the Internet through the predefined access point.
2. Mobile Security will prompt you if you need to restart the device. Restart the device when prompted.



Trend Micro strongly recommends performing a manual scan immediately after updating the program components. For more information on performing a manual scan, see [Manual Scan](#) on page 5-2.

Scanning for Viruses

Trend Micro Mobile Security scans your device for mobile viruses and other malware. It can also detect certain spyware/grayware applications and files that take advantage of vulnerabilities in your device. Read this chapter to understand the antivirus features of Mobile Security.

This chapter covers the following topics:

- *Antivirus Scan Types* on page 5-2
- *Manual Scan* on page 5-2
- *Real-time Scan* on page 5-3
- *Card Scan* on page 5-4
- *Scan Results* on page 5-5
- *Quarantined Files* on page 5-7
- *Advanced Antivirus Settings* on page 5-8
- *Information on Mobile Viruses* on page 5-10

5 Antivirus Scan Types

Mobile Security offers the following antivirus scan types:

Scan Type	Description
Manual scan	On-demand, user-initiated scan
Real-time scan	Automatic scan of files that are being accessed
Card scan	Automatic scan of memory cards when they are inserted

TABLE 5-1. Antivirus scan types

Manual Scan

A manual scan will scan all memory on your device for viruses and other malware. To run a manual scan, select **Options > Scan** on the main screen.

The scan results screen displays a list of any detected and unscannable files. You can choose to delete or quarantine these files. For more information, see *Handling detected or unscannable files* on page 5-6.

Real-time Scan

When enabled, the real-time scanner will scan files as you or applications on your device access them. This scan prevents device users from inadvertently opening viruses and other malware.

Enabling real-time scan

Enabling real-time scan enhances virus protection on your device.

To enable real-time scan:

1. Select **Options > Settings > Scan settings** on the main screen. The **Scan settings** screen opens.
2. Scroll to **Real-time scan** and press the scroll key to select **Enabled**.



*To disable the real-time scanner, select **Disabled** under **Real-time scan** in the **Scan settings** screen. If you disable the real-time scanner, your device will be unprotected against viruses and other malware.*



Figure 5-1. Scan settings screen

Setting the action on detected files

By default, the real-time scan automatically quarantines (encrypts and moves) detected files. However, you can configure the real-time scan to automatically delete detected files or prevent the applications from accessing the files.

To select your preferred real-time action, scroll to **Default action** and press the scroll key to select from the following options:

- **Quarantine**—encrypts and moves the files to prevent inadvertent access; quarantined files can be restored
- **Delete**—removes the files permanently from your device
- **Deny access**—prevents users and applications from accessing the files

Card Scan

Enable the card scan, which is disabled by default, to automatically check memory cards for viruses and other malware. When the card scan is enabled, inserting a memory card into your device triggers the scan.

To enable card scan:

1. **Options > Settings > Scan settings** on the main screen. The **Scan settings** screen opens.
2. Scroll to **Instant card scan** and press the scroll key to select **Enabled**.

Scan Results

Mobile Security displays scan results for card and manual scans, allowing you to specify an action for each detected or unscannable file.

Viewing scan results

After a manual or card scan, Mobile Security displays a list of detected and unscannable files. You can either quarantine or delete these files as discussed in *Handling detected or unscannable files* on page 5-6.

Scan result items can either be detected files or unscannable files as shown in the table below.

Scan Result Item	Description
Detected files	Files found to contain mobile viruses/malware
Unscannable files	Files compressed within an archive that cannot be accessed; these files may be compressed within too many layers of compression, password-protected, or too large to be extracted on the device

TABLE 5-2. Scan result items



Figure 5-2. Scan results screen

To view details on a detected or unscannable file, scroll to the file and press the scroll key.



For more information on setting the number of compression layers to scan, see [Advanced Antivirus Settings](#) on page 5-8.

Handling detected or unscannable files

If you exit the scan results screen without quarantining or deleting detected files, these potentially harmful files will stay intact and will be able to affect your device.

To delete or quarantine a detected or unscannable file:

1. On the scan results screen, scroll to a detected or an unscannable file.
2. Select **Options** and then select any of the following actions:
 - **Delete**—permanently remove the detected or unscannable file from your device
 - **Quarantine**—encrypt and move the detected or unscannable file to a quarantine folder



*To quarantine or delete all detected files, select **Delete All** or **Quarantine All**. These commands do not affect unscannable files.*

Quarantined Files

You can access quarantined files on the **Quarantine** screen. The screen lists files automatically quarantined during real-time scan or files that you have manually quarantined after a manual or a card scan.

To open the list, select **Options > Quarantine list** on the main screen.

To access quarantined files like normal files, restore them to their original state. If you restore quarantined files, you will expose your device to potentially harmful files.

To restore files from quarantine:

1. On the **Quarantine** screen, scroll to the file you wish to restore.
2. Select **Options > Restore**.



Trend Micro recommends that you do not open detected files after restoring them, unless you are certain they are safe.



Figure 5-3. Quarantine list

Advanced Antivirus Settings

You can specify the maximum number of compression layers (up to three) that Mobile Security will support before considering compressed files unscannable.

Scanning compressed files

When scanning compressed (ZIP/SIS) files, Mobile Security first extracts the files. As a result, Mobile Security requires more time and resources to scan compressed files.

You can set Mobile Security to extract files from within up to three compression layers. If a file is compressed in more layers than you have set, Mobile Security will consider the file unscannable.

Before deciding on the number of compression layers, consider the following:

- You are unlikely to inadvertently open files within multiple compression layers.
- Unless you knowingly prepare or use files in multiple compression layers, most such files you encounter likely have been prepared to elude antivirus scanners. Although such files may not be scanned if you select a low maximum number of compression layers, they will be tagged unscannable and you will be able to delete or quarantine them.

Configuring scan settings for compressed files

Configure the compression layers to scan in the **Scan settings** screen.

To configure the compression layers to scan:

1. From the main menu, select **Options > Settings > Scan settings**.
2. Scroll to **ZIP/SIS scan level** and press the scroll key to select the number of ZIP and SIS compression layers to scan.
3. Select **OK**.



*The item **Default action** applies only to the real-time scan. See [Setting the action on detected files](#) on page 5-4.*

Information on Mobile Viruses

To view information on known mobile viruses, select **Options > Virus definitions** on the main screen. The **Virus definitions** screen opens as shown in Figure 5-4.

To view additional details on a virus, scroll to the name of the virus and press the scroll key.



Figure 5-4. Virus definitions screen

Using the Firewall

The Trend Micro Mobile Security firewall allows you to filter incoming and outgoing network traffic. Read this chapter to understand how the firewall can protect your device.

This chapter covers the following topics:

- *Understanding Firewalls* on page 6-2
- *Understanding Mobile Security Firewall Filtering* on page 6-2
- *Enabling the Firewall* on page 6-6
- *Configuring the Firewall Protection Level* on page 6-6
- *Advanced Firewall Settings* on page 6-7

Understanding Firewalls

Firewalls control access to ports on network-connected computers and devices. With the Mobile Security firewall, you can control which ports external applications can use to connect to your device. You can control the ports that applications running on your device can use to connect to external systems. In addition to controlling access to ports, you can control which IP addresses can connect to your device and the addresses to which your device can connect.

A firewall boosts security on your network-connected device by preventing unwanted connections initiated by external systems or applications running on your device. For example, to prevent a hacker from accessing your device through a particularly vulnerable port, you can block that port.



Ports are typically associated with certain applications and services. See [Firewall rules](#) on page 6-4 for more information.

Understanding Mobile Security Firewall Filtering

Mobile Security provide two filtering methods with the firewall:

- Predefined protection levels
- Firewall rules

Predefined protection levels

The predefined protection levels (shown in Table 6-1) allow you to quickly configure your firewall. Each level corresponds to a general rule by which Mobile Security treats inbound and outbound connections.

Protection Level	Mode	Description
Low	Open	All inbound and outbound traffic is allowed.
Medium	Stealth	All outbound traffic is allowed; all inbound traffic is blocked.
High	Locked	All inbound and outbound traffic is blocked.

TABLE 6-1. Predefined protection levels



Because firewall rules take precedence over the predefined protection levels, adjusting the protection level changes only how Mobile Security treats network communication that is not covered by the firewall rules.

Firewall rules

Firewall rules define protection settings for specific ports and IP addresses. These rules take precedence over the predefined protection levels. Mobile Security lists current firewall rules in the **Firewall rule list** screen as shown in Figure 6-1.

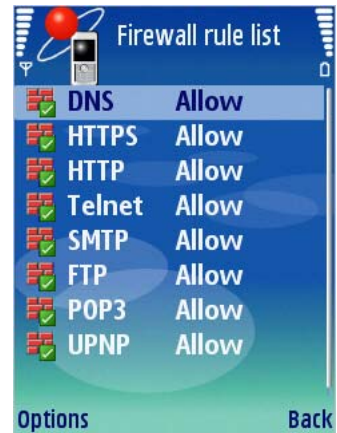


Figure 6-1. Firewall rule list

Mobile Security provides a set of default firewall rules that cover common ports used for functions like Web browsing and email. Table 6-2 lists the default firewall rules.

Rule	Port	Common Usage	Default Firewall Setting
DNS	53	Domain name resolution	Allows all inbound and outbound traffic through this port
HTTPS	443	Secure Web browsing	Allows all inbound and outbound traffic through this port
HTTP	80	Web browsing	Allows all inbound and outbound traffic through this port
Telnet	23	Server communication	Allows all inbound and outbound traffic through this port
SMTP	25	Email	Allows all inbound and outbound traffic through this port
FTP	21	File transfer	Allows all inbound and outbound traffic through this port
POP3	110	Email	Allows all inbound and outbound traffic through this port
UPnP	1900	Network connectivity	Allows all inbound traffic through this port

TABLE 6-2. Default firewall rules



You can modify the default firewall rules and create your own rules. For more information, see *Advanced Firewall Settings* on page 6-7.

6 Enabling the Firewall

To get firewall protection every time you connect to a network, enable the firewall.

To enable the firewall:

1. Select **Options > Settings > Firewall settings** on the main screen. The **Firewall settings** screen opens.
2. Scroll to **Firewall** and press the scroll key to select **Enabled**.

Configuring the Firewall Protection Level

The predefined protection levels allow you to quickly configure the Mobile Security firewall.



For details on the predefined protection levels, see [Predefined protection levels](#) on page 6-3.

To configure your firewall protection level:

1. Select **Options > Settings > Firewall settings** on the main screen.



Figure 6-2. Firewall settings screen

2. Ensure that **Firewall** is enabled.
3. Scroll to **Protection level** and press the scroll key to select your preferred protection level.
4. Select **OK**.



You can also select the firewall protection level on the main screen.

Advanced Firewall Settings

In addition to the predefined protection levels and the default rules, you can create your own rules and enable intrusion detection to enhance your firewall protection.

Creating firewall rules

Firewall rules will add custom filtering settings to your selected protection level. These rules will allow you to configure actions for specific ports, port ranges, specific IP addresses, subnets, and IP address ranges. For example, you can specify the IP address of a particular computer to allow all traffic between your device and that computer.

To create a firewall rule:

1. Select **Options > Settings > Firewall settings** on the main screen.
2. Ensure that **Firewall** is enabled.
3. Scroll to **Firewall rule list** and press the scroll key.
4. Select **Options > New rule**. The **Rule details** screen opens as shown in Figure 6-3.



*To duplicate existing firewall rules, select a rule and select **Options > Duplicate**.*

5. Provide a unique name for the rule.



Figure 6-3. Rule details screen

6. Provide the corresponding details on the **Rule details** screen. For information on the items on the screen, see Table 6-3.

Item	Options	Definition
Status	<ul style="list-style-type: none">• Enabled• Disabled	Turns the rule on or off
Action	<ul style="list-style-type: none">• Deny• Allow• Log only	Determines whether a connection attempt that matches the rule will be allowed, denied, or only logged
Direction	<ul style="list-style-type: none">• Inbound• Outbound• Both	Determines whether this rule applies to incoming or outgoing connections or both
Protocol	<ul style="list-style-type: none">• All• TCP/UDP• TCP• UDP• ICMP	Determines the network protocol to which this rule applies

TABLE 6-3. Rule details screen items

Item	Options	Definition
Port(s)	<ul style="list-style-type: none"> • All ports • Port range • Specific port(s) 	<p>Determines the ports in the device (for incoming connections) or remote system (for outgoing connections) where access is allowed or denied; you can allow or deny access to all network ports, a port range, or up to 32 specific ports</p> <p>When specifying ports, separate each port with a comma.</p> <p>Note: When ICMP or All is selected under Protocol, you cannot specify ports.</p>
IP address(es)	<ul style="list-style-type: none"> • All IP addresses • Single IP • IP range • Subnet 	<p>Determines the IP addresses to which access is allowed or denied; you can allow or deny access to all IP addresses, a specific IP address, an IP address range, or a subnet</p> <p>Note: To apply the rule to a subnet, you must specify a network IP address and a subnet mask.</p>

TABLE 6-3. Rule details screen items (continued)

7. Select **Back**.

Setting firewall rule list order

Firewall rules may overlap when they cover the same ports or IP addresses. When they do, rules on top of the list take precedence over rules that are closer to the bottom.

To move a rule up or down the list:

1. Select **Options > Settings > Firewall settings** on the main screen.
2. Ensure that **Firewall** is enabled.
3. Scroll to **Firewall rule list** and press the scroll key.
4. Scroll to a rule and then select **Options > Move**. To indicate the location of the rule, the **Firewall rule list** screen displays a move pointer as shown in Figure 6-4.
5. Scroll to move the rule to your preferred location.
6. Select **OK**.



Avoid creating rules that cover multiple ports and multiple IP addresses. Firewall rules that cover specific ports or specific IP addresses are easier to manage and are less likely to overlap.

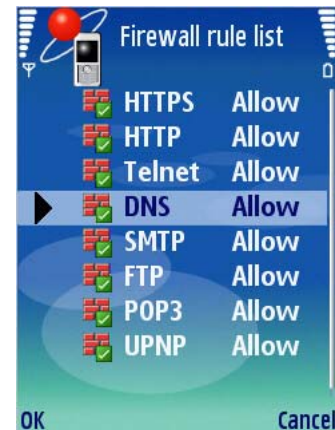


Figure 6-4. Firewall rule list with move pointer

Deleting firewall rules

Delete unwanted rules to prevent them from cluttering your rule list.

To delete a firewall rule:

1. Select **Options > Settings > Firewall settings** on the main screen.
2. Ensure that **Firewall** is enabled.
3. Scroll to **Firewall rule list** and press the scroll key.
4. Scroll to the rule and select **Options > Delete**. A confirmation prompt opens.
5. Select **Yes** on the confirmation prompt.



*To disable a firewall rule without deleting it, open the rule and select the status **Disabled** on the **Rule details** screen.*

Enabling intrusion detection

An intrusion detection system (IDS) is built into the Mobile Security firewall. Use the IDS to block attempts by external sources to continuously send multiple packets to your device. Such attempts typically constitute a denial of service (DoS) attack and can render your device too busy to accept other connections.

To enable intrusion detection:

1. Select **Options** > **Settings** > **Firewall settings** on the main screen.
2. Ensure that **Firewall** is enabled.
3. Scroll to **IDS** and press the scroll key to select **Enabled**.



The IDS will block only SYN flood attacks, which it detects when a remote system makes successive connection requests.

Filtering SMS Messages

Trend Micro Mobile Security lets you filter unwanted SMS messages into a Spam folder. Read this chapter to learn how to configure SMS message filtering.

This chapter covers the following topics:

- *SMS Anti-spam Filter Types* on page 7-2
- *SMS Anti-spam Configuration* on page 7-3
- *Handling Blocked SMS Messages* on page 7-10

SMS Anti-spam Filter Types

To filter SMS messages, you can use either of the following filtering lists:

- **Approved list**—when enabled, Mobile Security will block all messages except messages from phone numbers on this list.
- **Blocked list**—when enabled, Mobile Security will allow all messages except messages from phone numbers on this list.



*Mobile Security will move all blocked SMS messages to a Spam folder in your inbox.
For more information, see [Handling Blocked SMS Messages](#) on page 7-10.*

SMS Anti-spam Configuration

To configure anti-spam settings, select **Options > Settings > SMS anti-spam** on the main screen. The **SMS anti-spam settings** screen opens as shown in Figure 7-1.

Enabling SMS anti-spam filtering

To filter unwanted SMS messages, enable either the approved list or the blocked list.

- If you want to receive messages only from a list of known phone numbers, enable the approved list.
- If you want to block messages from specific users and accept all other messages, enable the blocked list.

To enable an anti-spam filtering list:

1. Select **Options > Settings > SMS anti-spam** on the main screen.
2. Scroll to **Anti-spam setting** and press the scroll key to select either **Use approved list** or **Use blocked list**. Mobile Security displays the selected filtering list as soon as you enable it.



Figure 7-1. SMS anti-spam settings screen

Adding senders to your anti-spam list

There are two methods to add senders to your anti-spam list:

- Manually enter sender details
- Import senders from your device's contact list

To manually enter sender details:

1. Select **Options > Settings > SMS anti-spam** on the main screen.
2. Ensure that an anti-spam list is enabled.
3. Scroll to **Approved/Blocked list** and press the scroll key. Mobile Security displays the current list entries as shown in Figure 7-2.
4. Select **Options > New entry**.



Figure 7-2. SMS anti-spam approved list

A new screen opens as shown in Figure 7-3.

5. Enter the name and number of the sender.
6. Select **OK** to go back to the sender list. The entry appears on the list.

To import senders from your device's contact list:

1. Select **Options > Settings > SMS anti-spam** on the main screen.
2. Ensure that an anti-spam list is enabled.
3. Scroll to **Approved/Blocked list** and press the scroll key. Mobile Security displays the current list entries.
4. Select **Options > Import**.



Figure 7-3. SMS anti-spam approved list entry

The **Import** screen opens as shown in Figure 7-4.

5. Select the contacts to import by:
 - Scrolling to a contact and pressing the scroll key
 - Choosing all contacts by selecting **Options** > **Select all**
6. Select **Options** > **Import**.
7. Verify that your contacts have been imported.

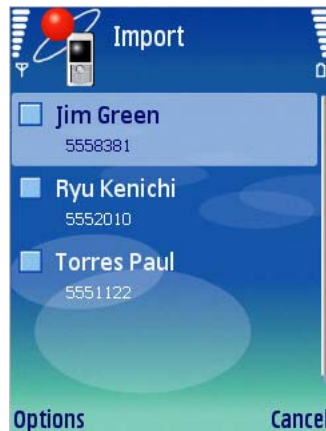


Figure 7-4. Import screen

Editing information on senders in your anti-spam list

Edit listed senders in your anti-spam list to change the senders' names or phone numbers.

To edit sender information:

1. Select **Options** > **Settings** > **SMS anti-spam** on the main screen.
2. Ensure that an anti-spam list is enabled.
3. Scroll to **Approved/Blocked list** and press the scroll key. Mobile Security displays the current list entries.
4. Scroll to the name of the sender.
5. Select **Options** > **Edit**.
6. Modify the sender information and select **OK**.

Deleting senders from your anti-spam list

Check whether you have enabled the approved or the blocked list before deleting senders from your anti-spam filtering list.

- If you delete a sender from the anti-spam filtering list with the approved list enabled, you will block SMS messages from the sender.
- If you delete a sender from your anti-spam filtering list with the blocked list enabled, you will allow SMS messages from the sender.

To delete a sender:

1. Select **Options > Settings > SMS anti-spam** on the main screen.
2. Ensure that an anti-spam list is enabled.
3. Scroll to **Approved/Blocked list** and press the scroll key. Mobile Security displays the current list entries.
4. Scroll to the name of the sender.
5. Select **Options > Delete**.



*To delete multiple senders simultaneously, use the **Mark/Unmark** options to choose the senders and then select **Options > Delete**.*

6. A confirmation prompt appears. Select **Yes**.

Blocking SMS messages from unidentified senders

When the blocked list is enabled, you can block SMS messages that do not carry sender number information.

To block messages from unidentified senders:

1. Select **Options > Settings > SMS anti-spam** on the main screen.
2. Ensure that **Use blocked list** is selected under **Anti-spam setting**.

3. Scroll to **Block unknown SMS** and press the scroll key to select **Enabled** as shown in Figure 7-5.



Blocking SMS messages that do not have sender number information may filter out messages that you want to receive. Check the Spam folder periodically to ensure that the current SMS anti-spam settings do not block messages that you want to receive. See [Handling Blocked SMS Messages](#) on page 7-10.



Figure 7-5. SMS anti-spam with Block unknown SMS enabled

Disabling SMS anti-spam filtering

To let all SMS messages reach your inbox, disable SMS filtering.

To disable all SMS filtering:

1. Select **Options** > **Settings** > **SMS anti-spam** on the main screen.
2. Scroll to **Anti-spam setting**.
3. Press the scroll key and select **Disable anti-spam**.
4. Click **OK**.

Handling Blocked SMS Messages

Mobile Security moves blocked SMS messages to a **Spam** folder inside the **My folders** folder (shown in Figure 7-6). You can handle these messages as you would messages in the **Inbox** folder.

To access messages in the Spam folder:

1. Go to **Menu > Messaging**.
2. Scroll to **My folders** and press the scroll key.
3. Scroll to **Spam** and press the scroll key.

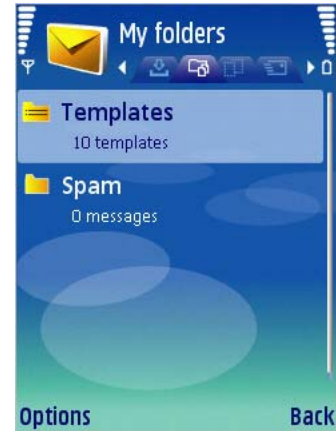


Figure 7-6. Spam folder

Filtering WAP Push Messages

WAP Push messages can initiate the delivery of unwanted content to your device. Read this chapter to learn how Trend Micro Mobile Security can help block unwanted WAP Push messages.

This chapter covers the following topics:

- *Understanding WAP Push Messages* on page 8-2
- *Enabling WAP Push Protection* on page 8-3
- *Enabling WAP Push Notification* on page 8-3
- *Managing the WAP Push Trusted Senders List* on page 8-4
- *Handling Blocked WAP Push Messages* on page 8-7

Understanding WAP Push Messages

WAP Push is a powerful method of delivering content to handheld devices automatically. It may be used to deliver mobile-related content such as ringtones, news, email, and device settings. Because of this ability to deliver content to handheld devices, WAP Push can deliver unsolicited or unwanted content, including viruses and advertisements.

To initiate the delivery of content, special SMS messages called WAP Push messages are sent to users. These messages typically display an alert on your device as soon as you receive them. These alerts give you the option to connect directly to a WAP site and download content into your device.

Malicious users have been known to send out inaccurate or uninformative WAP Push messages to trick users into accepting unwanted content. By blocking WAP Push messages from unknown senders, you can avoid inadvertently downloading and installing unwanted WAP Push content.

Enabling WAP Push Protection

WAP Push protection allows you to use a list of trusted senders to filter WAP Push messages.

To enable WAP Push protection:

1. Select **Options > Settings > WAP Push protection** on the main screen. The **WAP Push protection** settings screen opens as shown in Figure 8-1.
2. Scroll to **WAP Push protection** and press the scroll key to select **Enabled**.



Figure 8-1. WAP Push protection settings screen

Enabling WAP Push Notification

Instead of automatically blocking WAP Push messages from unknown senders, Mobile Security can alert you so that you can accept or block the messages.

To enable WAP Push notification:

1. Select **Options > Settings > WAP Push protection** on the main screen. The **WAP Push protection** settings screen opens.
2. Ensure that **WAP Push protection** is enabled.
3. Scroll to **WAP Push notification** and press the scroll key to select **Enabled**.

Managing the WAP Push Trusted Senders List

Mobile Security will automatically allow WAP Push messages from senders on your trusted list and block messages from unknown senders, unless you enable WAP Push notification. With the notification enabled, Mobile Security will prompt you to allow or block message from unknown senders.

Adding trusted WAP Push senders

If you frequently receive WAP Push messages from the same phone numbers, add these numbers to your trusted senders list.

To add a sender to the trusted senders list:

1. Select **Options > Settings > WAP Push protection** on the main screen. The **WAP Push protection** settings screen opens.
2. Ensure that **WAP Push protection** is enabled.
3. Scroll to **Trusted list** and press the scroll key.

The trusted list appears displaying current entries as shown in Figure 8-2.

4. Select **Options** > **New Entry**.
5. Enter the name and number of the sender.
6. Select **OK**.



*Alternatively, to add a WAP Push sender to your trusted list, select **Accept** whenever Mobile Security alerts you to a WAP Push message and then choose to add the sender when prompted. For information on enabling these alerts, see [Enabling WAP Push Notification](#) on page 8-3.*



Figure 8-2. WAP Push trusted list

Modifying information on trusted WAP Push senders

To edit trusted sender information:

1. Select **Options** > **Settings** > **WAP Push protection** on the main screen. The **WAP Push protection** settings screen opens.
2. Ensure that **WAP Push protection** is enabled.
3. Scroll to **Trusted list** and press the scroll key.
4. Scroll to the entry to edit.

5. Select **Options > Edit**.
6. Modify the sender information and select **OK**.

Deleting trusted WAP Push senders

To delete senders from the trusted list:

1. Select **Options > Settings > WAP Push protection** on the main screen. The **WAP Push protection** settings screen opens.
2. Ensure that **WAP Push protection** is enabled.
3. Scroll to **Trusted list** and press the scroll key.
4. Scroll to the entry to delete.
5. Select **Options > Delete**.



*To delete multiple senders simultaneously, use the **Mark/Unmark** options to choose the senders and then select **Options > Delete**.*

6. Select **Yes** on the confirmation prompt.

Handling Blocked WAP Push Messages

With WAP Push notification enabled, Mobile Security alerts you whenever you receive a WAP Push message from a sender that is not on your trusted list. Figure 8-3 shows the WAP Push alert message.

Select **Reject** on the message to prevent the WAP Push messages from reaching your device. These blocked messages will not be stored on your device.

Select **Accept** to accept the message. After you accept the WAP Push message, Mobile Security prompts you to add the message sender to your trusted list.



For information on enabling WAP Push notification, see [Enabling WAP Push Notification](#) on page 8-3.



Figure 8-3. WAP Push alert message

Viewing Event Logs

Event logs contain information on detected files, scan and update results, filtered SMS and WAP Push messages, and blocked connection attempts. Read this chapter to understand the types of Trend Micro Mobile Security event logs and to learn how to use these logs.

The chapter covers the following topics:

- *Event Log Types* on page 9-2
- *Viewing Logs* on page 9-12
- *Deleting Logs* on page 9-13

9 Event Log Types

Mobile Security maintains event logs, which you can use to track product activities and view task results. Mobile Security supports the following log types:

- *Scan log* on page 9-2
- *Task log* on page 9-4
- *Firewall log* on page 9-6
- *Spam log* on page 9-8
- *WAP Push log* on page 9-10

Scan log

Mobile Security generates an entry in the scan log (shown in Figure 9-1) every time it detects a virus or other malware.

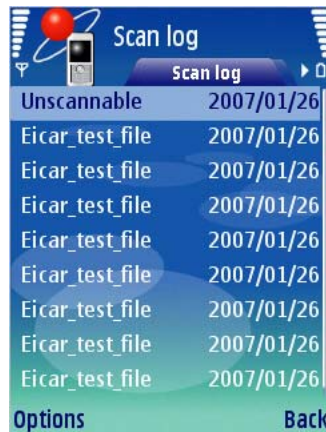


Figure 9-1. Scan log entries

Each scan log entry (shown in Figure 9-2) contains the following information:

- **Found**—when the virus was detected
- **Risk name**—the name of the virus
- **File**—the name of the detected file
- **Action**—whether the file was quarantined or deleted
- **Result**—whether the action was successfully completed

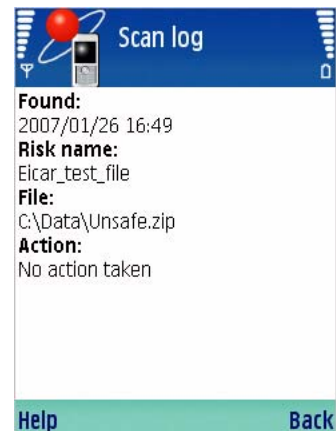


Figure 9-2. Scan log entry details

Task log

Mobile Security generates an entry in the task log (shown in Figure 9-3) every time it runs a manual scan, a card scan, or an update.



Figure 9-3. Task log entries

Each task log entry (shown in Figure 9-4) contains the following information:

- **Started**—when the task was started
- **Ended**—when the task was completed
- **Task**—whether a scan or an update was performed
- **Files scanned**—the number of files checked for viruses (scan tasks only)
- **Suspicious files**—the number of files found with viruses (scan tasks only)
- **Files not scanned**—the number of files skipped for scanning (scan tasks only)
- **Result**—whether the task was successfully completed

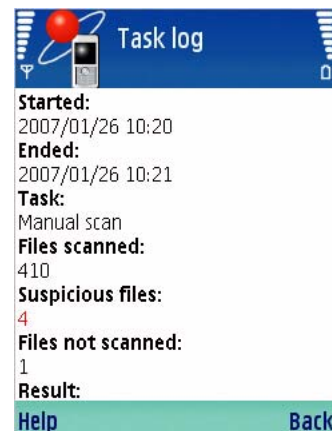


Figure 9-4. Task log entry details

Firewall log

Mobile Security generates an entry in the firewall log (shown in Figure 9-5) every time a connection attempt matches a firewall rule or when the predefined protection level or the IDS blocks a connection attempt.



Figure 9-5. Firewall log entries

Each firewall log entry (shown in Figure 9-6) contains the following information:

- **Type**—event type, firewall or IDS
- **Date and time**—when the connection attempt was made
- **Action**—whether the connection was allowed or blocked
- **Protocol**—the layer 4 protocol used by the connection
- **Direction**—whether the connection was inbound or outbound
- **Source IP**—the IP address that requested the connection
- **Destination IP**—the IP address that received or was supposed to receive the connection
- **Destination Port**—the port used for the connection
- **Description**—whether a firewall rule or predefined protection was applied; for IDS, indicates the type of attack



Figure 9-6. Firewall log entry details

Spam log

Mobile Security generates an entry in the spam log (shown in Figure 9-7) every time it blocks an SMS message.



Figure 9-7. SMS anti-spam log entries

Each spam log entry (shown in Figure 9-8) contains the following information:

- **Received**—when the message arrived
- **Sender**—the number of the message sender
- **Type**—the message type (SMS)
- **Result**—whether the message was successfully blocked

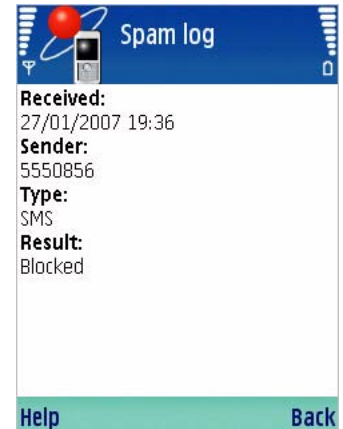


Figure 9-8. SMS anti-spam log entry details

9

WAP Push log

Mobile Security generates an entry in the WAP Push log (shown in Figure 9-9) every time it blocks a WAP Push message.



Figure 9-9. WAP Push log entries

Each WAP Push log entry (shown in Figure 9-10) contains the following information:

- **Received**—when the message arrived
- **Sender**—the number of the message sender
- **Type**—the message type (WAP Push)
- **Result**—whether the message was successfully blocked



Figure 9-10. WAP Push log entry details

9

Viewing Logs

To view each log, select the log from the **Event logs** submenu.

To view log entries:

1. Select **Options > Event logs** and then select the log type. Figure 9-11 shows the log types in the **Event logs** submenu.
2. In the log screen, scroll to the log entry you wish to view.
3. Press the scroll key.

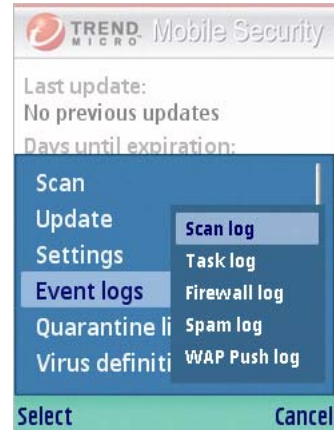


Figure 9-11. Event logs submenu

Deleting Logs

To delete the entries in a log, clear the entire log.

To clear a log:

1. Select **Options** > **Event logs** and then select the log type.
2. Select **Options** > **Clear log**.
3. Select **Yes** on the confirmation prompt.



Mobile Security allocates 16KB of memory space for each log type. When this limit is reached, it automatically deletes the oldest entries to accommodate new entries.

Troubleshooting, FAQ, and Technical Support

You may encounter some problems while using Trend Micro Mobile Security. Read this chapter for a list of common problems and workarounds and instructions on how to contact technical support.

This chapter covers the following topics:

- *Troubleshooting* on page 10-2
- *Frequently Asked Questions (FAQ)* on page 10-4
- *Technical Support* on page 10-7
- *About TrendLabs* on page 10-10
- *About Trend Micro* on page 10-11

Troubleshooting

The following section provides methods for addressing issues that may arise when installing, configuring, or using Mobile Security.

Issue	Recommended Action
The device encountered a battery failure while installing Mobile Security. The installation process was stopped.	Ensure that the device has adequate power and perform the installation process again.
My battery failed while uninstalling Mobile Security. Subsequent installation efforts would always fail.	Uninstallation did not complete. Use available tools designed for your device to remove incomplete software installations.
I cannot open quarantined files.	When Mobile Security quarantines a file, it encrypts the file. You may restore the quarantined file; however, Trend Micro does not recommend this action.
Mobile Security is operating slowly.	Check the amount of storage space available on the device. If you are approaching the device's maximum memory limit, consider deleting unnecessary files and applications.
I cannot perform updates while the device is connected to a host computer.	Verify the following: <ul style="list-style-type: none"> • The device's proxy settings are identical to the host computer's settings • The host computer is connected to the Internet

Issue	Recommended Action
<p>I cannot receive SMS messages after installing Mobile Security.</p>	<p>If the approved senders list is enabled and the list is empty, all SMS messages will be blocked and moved to the Spam folder. Check the Spam folder and your anti-spam settings.</p>
<p>I cannot receive WAP Push messages even when I choose to accept the messages.</p>	<p>Your device or service may not support receiving WAP Push messages. Check your device's documentation or contact your service provider to find out whether you can receive WAP Push messages.</p>
<p>A message pops up that requests to open a wireless connection.</p>	<p>This is normal if you have selected the Connection alert option in the Update settings screen. You can disable this option, but you will not be warned whenever Mobile Security opens a wireless connection to check for updates.</p>
<p>Mobile Security has been installed successfully. However, a security risk being copied could not be detected.</p>	<p>Verify that the Activation Code has not expired. Also, Trend Micro recommends opening the Mobile Security main screen after installation to ensure that all modules are loaded. Visit the Trend Micro Web site at http://www.trendmicro.com/tmms/buy for AC registration details.</p>

Issue	Recommended Action
I cannot copy a file into the device.	The file may be infected and is being blocked by Mobile Security. You can disable Real-time Scan, but you will risk infecting your device.
I cannot access the Internet or other network resources.	Check your firewall settings. If the firewall protection level is set to High , all inbound and outbound traffic will be blocked. See <i>Using the Firewall</i> on page 6-1.
I cannot use the firewall or the WAP Push protection feature.	Try restarting your device. Mobile Security requires a restart after installation to load the firewall or the WAP Push protection driver.

Frequently Asked Questions (FAQ)

- **Can I install Mobile Security on a storage card?**
No. Mobile Security can only be installed into your device's internal memory.
- **How long can I use Mobile Security and download program and virus pattern file updates?**
You can check the expiration date of your license by selecting **Options > About** on the main screen.

- **Can I download virus pattern files to a storage card even though Mobile Security is installed directly on the device?**
No. The virus pattern files are downloaded and installed to the same location where you installed Mobile Security.
- **How often should I update Mobile Security program components?**
Trend Micro recommends updating program components weekly.
- **Can Mobile Security scan compressed files?**
Yes. Mobile Security can scan ZIP and SIS files. You can configure Mobile Security to scan within up to three compression layers.
- **Can I receive or make a call while Mobile Security is performing a scan?**
Yes. Mobile Security can scan in the background while you perform other functions on the device. You can view the logs to see details on scans and any detected viruses and security risks.
- **Can I clean detected security risks?**
No. Mobile Security can only quarantine or delete infected files.
- **Will Mobile Security log entries take up a large amount of memory space?**
Mobile Security allows each type of log a maximum of 16KB of memory.
- **Can I open detected files on my device?**
With real-time scan enabled, Mobile Security will block the opening, copying, or moving of any detected security risks. You may disable real-time scan, but you will risk infecting your device.

- **Can Mobile Security detect a mixed-compression file (for example, a ZIP file containing an SIS file)?**

Yes. Mixed-compression scanning is supported in Mobile Security.

- **Can a quarantined file be opened again?**

Mobile Security encrypts quarantined files to prevent users from inadvertently opening the file. You may restore the quarantined file; however, Trend Micro does not recommend this action.

- **How does Mobile Security match sender numbers to my SMS anti-spam filtering and WAP Push trusted lists?**

Mobile Security uses either partial or full matching to check sender numbers against your lists. When the sender number has seven or more digits, Mobile Security uses only the last seven digits to check the number against listed numbers with at least seven digits. When the sender's number is less than seven digits, it uses full matching. During full matching, both numbers have to have exactly the same digits.

- **Can I install Mobile Security with other security products?**

Trend Micro cannot guarantee compatibility between Mobile Security and file system encryption software. Software products that offer similar features, such as antivirus scanning, SMS management, and firewall protection, may also be incompatible with Mobile Security.

- **Can I extend the license of my installation copy?**

Yes. You can apply to renew your Activation Code to extend your license. Visit the Trend Micro Web site at <http://www.trendmicro.com/tmms/buy> for licensing details.

Technical Support

Trend Micro has sales and corporate offices located in many cities around the globe. For global contact information, visit the Trend Micro Web site at:

<http://www.trendmicro.com/en/about/contact/overview.htm>



The information on this Web site is subject to change without notice.

Contacting Technical Support

You can contact Trend Micro by fax, device, and email, or visit us at:

<http://www.trendmicro.com>

Speeding up your support call

When you contact Trend Micro Technical Support, to speed up your problem resolution, ensure that you have the following details available:

- Operating system and service pack versions for the host computer
- Network type
- Computer and device brand, model, and any additional hardware connected to your device

- Amount of memory and free space on your device
- Exact text of any error messages
- Steps to reproduce the problem

Using the Knowledge Base

The Trend Micro Knowledge Base is a 24x7 online resource that contains thousands of do-it-yourself technical support procedures for Trend Micro products. Use Knowledge Base, for example, if you are getting an error message and want to find out what to do. New solutions are added daily.

Also available in Knowledge Base are product FAQs, important tips, preventive antivirus advice, and regional contact information for support and sales.

All Trend Micro customers, including users of evaluation versions, can access Knowledge Base at:

<http://esupport.trendmicro.com/>

If you cannot find an answer to a particular question, Knowledge Base includes an additional service that allows you to submit your questions by email.

Sending security risks to Trend Micro

To send detected security risks and suspect files to Trend Micro for evaluation, visit the Trend Micro Submission Wizard at:

<http://subwiz.trendmicro.com/SubWiz>

When you click **Submit a suspicious file/undetected virus**, you will be prompted to supply the following information:

- **Email**—the email address where you would like to receive a response from the antivirus team
- **Product**—the Trend Micro product you are currently using; if you are using multiple products, select the most relevant product or the product you use the most
- **Upload File**—Trend Micro recommends that you create a password-protected zip file (using the password `virus`) to contain the suspicious file; you can then select the password-protected zip file for upload.
- **Description**—include a brief description of the symptoms you are experiencing; our team of virus engineers will analyze the file to identify and characterize any security risks it may contain

When you select **Next**, an acknowledgement screen displays. This screen also displays a case number that you can use to track your submission.

If you prefer to communicate by email message, send a query to virusresponse@trendmicro.com.

In the United States, you can also call the following toll-free telephone number: (877) TRENDAY, or 877-873-6328.



Submissions made through the submission wizard or the virus response mailbox are addressed promptly, but are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

About TrendLabs

TrendLabs is the Trend Micro global infrastructure for antivirus research and product support.

TrendLabs *virus doctors* monitor potential security risks around the world to ensure that Trend Micro products remain secure against emerging security risks. The culmination of these efforts is shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs involves a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located worldwide to mitigate outbreaks and provide urgently-needed support.

The modern TrendLabs headquarters was one of the first antivirus research and support facilities to earn ISO 9002 certification.

About Trend Micro

Trend Micro Incorporated provides virus protection, anti-spam, and content-filtering security products and services. Trend Micro allows companies worldwide to stop viruses and other malicious code from a central point before they can reach the desktop.

Glossary

Terminology	Definition
ActiveUpdate	the technology that Trend Micro products use to properly download and install updates from Trend Micro servers
anti-spam	technology designed to filter unwanted content as it is received by a messaging application or platform
antivirus	technology designed to detect and handle viruses and other malware
card scan	a Trend Micro Mobile Security feature that automatically scans inserted memory cards for viruses and other malware
CDMA2000™	a family of high-speed wireless communication standards based on Code Division Multiple Access (CDMA) technology; like GPRS, mobile providers typically offer services based on CDMA2000 standards for email and Web browsing
detected files	files that have been found to contain viruses and other malware
event logs	logs containing the results of product functions

Terminology	Definition
filtering	the process of distinguishing and handling unwanted content
firewall	an application or device that controls access to ports to regulate network communication to and from a computer or device
firewall rules	sets of information that instruct a firewall how to control access to ports
GPRS	General Packet Radio Service; a common standard for wireless communication typically offered by mobile providers for email and Web browsing
IDS	Intrusion detection system; technology designed to determine whether network activity constitutes an attack and to mitigate the effects of that attack
malware	a general term that refers to all kinds of malicious applications such as viruses and Trojans
pattern	see <i>virus pattern</i>
PC Suite	application that allows computers to connect and communicate with a handheld device running Symbian OS. S60 is a platform running on of Symbian OS
port	the endpoint of a logical rather than physical network connection. Ports are numbered such that each number refers to a type of logical connection. For example, when a firewall blocks a certain port number, it is actually blocking a type of logical connection

Terminology	Definition
real-time scan	a scanner that is always on and is triggered whenever an application accesses a file
scan	the process of determining whether a file or a set of files contain viruses or other malware
scan engine	the antivirus component that determines whether a file is a virus or other malware. The scan engine typically matches files with a collection of malware code snippets known as a <i>virus pattern</i>
security risks	a general term used to refer to files that can adversely affect computers or devices and their normal use
SMS	short message service; a common platform for sending text-based messages to and from mobile phones
SYN flood	a form of denial-of-service attack wherein the attacker sends multiple SYN packets, which are commonly used to request connections, to tie up the resources of the receiving computer or device
unscannable files	compressed files that Mobile Security cannot access and scan because they are either password-protected or are compressed under too many compression layers (see <i>Advanced Antivirus Settings</i> on page 5-8)
virus pattern	collection of malware code snippets that the scan engine uses as a basis for identifying malware

Terminology	Definition
virus	a kind of malware that can propagate by distributing copies of itself or by infecting other files or both
WAP	Wireless Application Protocol; this protocol is typically used to provide Web content to handheld devices, which often have limited network bandwidth, processing capabilities, and display space
WAP Push	automatic method of delivering content, such as applications and system settings, to handheld devices through the Wireless Application Protocol
WAP Push message	an SMS message that acts as a confirmation prompt prior to the delivery of WAP Push content

Index

A

- action on detected files 5-9
- Activation Code 2-6–2-7
- ActiveUpdate 4-2, G-1
- advanced settings 4-2
- anti-spam 1-5, 7-1, G-1
- antivirus 1-4, G-1
 - advanced settings 5-8
 - log 9-2
- approved list 7-2
- automatic updates 4-3

B

- blocked list 7-2
- blocked SMS messages 7-10
- blocked WAP Push messages 8-7
- blocking unidentified senders 7-8
- Bluetooth 1-3
- Bluetooth installation 2-4–2-5

C

- card scan 5-2, 5-4, G-1
- CDMA2000 G-1
- common ports 6-2
- compression layers 5-9

D

- default settings 3-6
- delete 5-4
- deny access 5-4
- detected files 5-5, G-1
- DNS 6-5
- DoS 1-2, 1-4

E

- event logs 1-6, 9-1, G-1
 - deleting 9-13
 - limit 9-13
 - types 9-2
 - viewing 9-12

F

- FAQ 10-4
- filtering G-2
- firewall 1-3–1-4, 6-1, 6-6, G-2
 - advanced settings 6-7
 - default rules 6-5
 - deleting rules 6-12
 - enabling 6-6
 - log 9-6
 - predefined protection levels 6-2

rule details 6-9
rule list 6-11
rules 6-2, 6-7
firewall rules G-2
firewalls 6-2
forced updates 4-3
FTP 6-5

G

getting started 3-1
GPRS G-2

H

handheld device requirements 2-2
host computer requirements 2-3
HTTP 6-5
HTTPS 6-5

I

IDS 1-4, 6-13, G-2
installation 2-4
Internet 4-2
intrusion detection system 6-13
IP address 6-7

K

Knowledge Base 10-8

L

license

purchase 2-4
types 2-7

M

main menu 3-5
main screen 3-4
malware G-2
manual scan 5-2
manual updates 4-3, 4-6
memory 2-2
Mobile Security
 features 1-3
 latest version 2-3
 overview 1-2
mobile threats 1-2, 5-10
mobile viruses 1-2, 5-10
move rule pointer 6-11

N

Nokia 2-2

O

operating system 2-2

P

pattern G-2
PC Suite 2-3, G-2
PC Suite installation 2-4
POP3 6-5

ports 6-7, G-2

predefined protection levels 6-6

Q

quarantine 5-4

quarantined files 5-7

R

real-time scan 5-2, G-3

 default action 5-4

 enabling 5-3

registration 2-6

S

S60 2-2

safe practices 1-3

scan G-3

scan engine G-3

scan log 9-2

scan results 5-5

 delete 5-6

 quarantine 5-6

scan types 5-2

scanning 3-3, 5-1

scheduled updates 4-3

security risks G-3

SIS files 5-9

SMS 1-2–1-3, 1-5, G-3

SMS anti-spam

 adding senders 7-4

 deleting senders 7-7

 disabling 7-9

 editing sender information 7-7

 enabling 7-3

 filter types 7-2

 log 9-8

SMS filtering 7-1

SMTP 6-5

spam 1-2

Spam folder 7-10

spam log 9-8

storage space 2-2

Submission Wizard 10-9

submitting suspicious files 10-9

subnet 6-7

supported devices 2-2

Symbian OS 2-2

SYN flood G-3

system requirements 2-2

T

task log 9-4

technical support 10-7

Telnet 6-5

Trend Micro 10-11

TrendLabs 10-10

troubleshooting 10-2

trusted senders list 8-4

- adding senders 8-4
- deleting senders 8-6
- modifying senders 8-5

U

- uninstallation 2-7
- unscannable files 5-5, G-3
- update types 4-3
- updates 1-4
- updating 3-2, 4-1
- UPnP 6-5
- user interface 3-3

V

- virus pattern G-3

- viruses G-4

W

- WAP G-4
- WAP Push 1-2, G-4
- WAP Push log 9-10
- WAP Push messages 1-3, 8-2, G-4
- WAP Push protection 1-5, 8-1
 - enabling 8-3
 - log 9-10
 - trusted senders list 8-4
- Windows 2-3

Z

- ZIP files 5-9