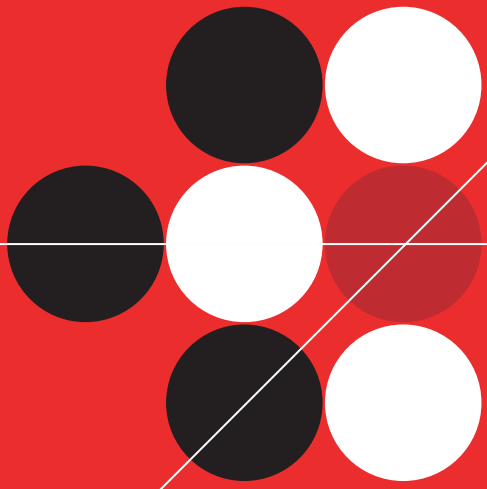
TREND MICRO™ Mobile Security

for Symbian™

UIQ 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 Trend Micro's Web site at:

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

Release Date: January, 2005

The User's Guide for Trend Micro Mobile Security is intended to introduce 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**. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

Contents

Index

Chapter 1

Introducing Trend Micro™ Mobile Security

This chapter provides an overview of how Trend Micro Mobile Security works and the features and functions it offers.

The topics in this chapter include the following:

Mobile Security Technology

Trend Micro™ Mobile Security for Symbian™ is an antivirus and spam prevention solution for mobile devices. It helps protect devices running the Symbian operating system from viruses and other threats, including unsolicited commercial messages (spam) sent by Short Messaging Service (SMS).

Understanding viruses

Tens of thousands of viruses exist. Although commonly designed to infect personal computers, viruses can also infect mobile devices. As people increasingly use mobile devices to share files, check email, and surf the Internet, the risk of infection increases.

Existing computer viruses include the following types:

- **ActiveX malicious code –** resides in Web pages that execute ActiveX controls
- **COM and EXE file infectors –** executable programs with .com or .exe extensions
- **Java malicious code** – operating-system-independent virus code written or embedded in Java
- **Macro viruses –** encoded as an application macro and often included in a document
- **Trojan horses –** executable programs that do not replicate but instead reside on systems to perform malicious acts, such as open ports for hackers to enter
- **HTML, VBScript, or JavaScript viruses –** reside in Web pages and are downloaded through a browser
- **Worms –** self-contained programs that are able to spread functional copies of themselves or their segments to other computer systems, often via email

Understanding Mobile Security antivirus components

Mobile Security uses the following antivirus components to scan for, identify, and delete infected files:

- **Client program:** the Mobile Security client program, which uses the Trend Micro virus pattern file and scan engine to identify infections and perform actions on infected files
- **Virus pattern file:** a file that helps Mobile Security identify virus signatures; unique patterns of bits and bytes that signal the presence of a virus (see *About the virus pattern file* on page 1-3 for more information)
- **Scan engine:** the program Mobile Security uses to scan for viruses. The scan engine is the heart of Mobile Security

About the virus pattern file

The Trend Micro scan engine uses an external data file, called the virus pattern file. It contains information that helps Mobile Security identify the latest viruses.

The scan engine works together with the virus pattern file to perform the first level of detection, using a process called pattern matching. Since each virus contains a unique “signature” or string of identifying characters that distinguish it from any other code, the virus experts at Trend Micro capture inert snippets of this code in the pattern file. The engine then compares certain parts of each scanned file to the pattern in the virus pattern file, looking for a match.

Pattern file numbering

To compare the virus pattern file on your device to the most current virus pattern file available from Trend Micro, check the file's version number.

To view the version number for your pattern file and other components:

- From the Mobile Security main screen, select **Mobile Security>About**.

The pattern file numbering system utilizes six digits, in the format *x.xxx.xx*.

- The first digit is currently set to 1, indicating the new numbering system
- The next 3 digits represent the primary pattern file number
- The last 2 digits provide additional information about the pattern file release for Trend Micro engineers

Keep the virus pattern file updated to the most current version to safeguard against the latest virus threats.

Mobile Security Features

Mobile Security includes the following features:

- Manual Scan, Real-time Scan, and Instant Card Scan for viruses
- Scan engine and virus pattern file update
- Anti-spam (SMS message filtering)
- Logs for virus detections, Anti-spam, and other tasks

Manual Scan, Real-time Scan, and Instant Card Scan

Mobile Security features the following types of scans:

- **Manual Scan** – allows you to initiate a scan of files on your device at any time
- **Real-time Scan** – automatically scans files whenever they are opened or executed
- **Instant Card Scan** – automatically scans a storage card when inserted into your device

Scan engine and virus pattern file update

To ensure that you stay protected against the latest threats, you must periodically update Mobile Security components. You can download updated components to your device via GPRS connection.

Anti-spam (SMS message filtering)

Unsolicited commercial messages, or spam, is often sent to mobile devices as SMS messages. You can filter unwanted SMS messages into a spam folder on your device. If you frequently receive spam from the same numbers, you can configure a list of phone numbers from which all SMS messages will be considered spam. You can also filter SMS messages from senders without a registered caller ID.

Logs for virus detection, Anti-spam, and other tasks

Analyze the logs to view details on detected viruses and suspicious files, filtered spam messages, antivirus component updates, and all scan results.

Chapter 2

Installing Mobile Security

This chapter provides instructions on installing Mobile Security.

The topics in this chapter include the following:

System Requirements

Before installing and using Mobile Security, ensure that your device meets the following system requirements:

Device requirements

Interface – UIQ 2.0 or 2.1

Operating system – Symbian OS 7.0

Storage space – 3MB minimum free in internal memory

Memory – 1MB minimum free memory, 2MB recommended

Host PC requirements

If you want to install using PC Suite software on a host PC for installation, the host PC needs to meet the following requirements:

Operating system - Microsoft™ Windows™ XP or Windows 2000

Using Your Device

See your device documentation for specific information on establishing a GPRS connection, and test your device's GPRS connection before performing an update.

Installing Mobile Security

Mobile Security provides two methods for installation:

- **PC Suite**– run the setup program using PC Suite software on a host PC connected to the phone
- **Bluetooth** – run the setup program directly on the phone after transferring it via Bluetooth

First, obtain the setup file from the included CD or other source provided to you by your vendor, or download it from the Trend Micro web site at **http://www.trendmicro.com**.

PC Suite

This section describes installation using PC Suite software on a host PC computer.

To install via PC suite:

1. Copy the setup file, `MobileSecurity_UIQ.sis`, to the host PC.
2. Connect your device to a host computer with PC Suite.
3. On the host computer, run the PC Suite software installation application. A prompt appears on the host PC.
4. Select the setup file and click **Open**. Installation begins.
5. Click **Install anyway** on the prompt that appears. A new prompt appears.
6. Click **Next**. A new prompt appears with language choices.
7. Select the correct language and click **Next**. The license agreement is displayed.

8. Carefully read the license agreement, and then click **Yes** if you want to continue installation. A prompt appears, informing you that Mobile Security can only be installed in internal memory.
9. Click **Yes**.
10. Click **Finish**. Installation is complete. **Mobile Security** now appears in your **Applications** menu.

Bluetooth

This section describes how to install by using Bluetooth to transfer the setup file to your phone.

To install via Bluetooth:

1. Copy the setup file, `MobileSecurity_UIQ.sis`, to a Bluetooth-enabled PC.
2. Transfer the setup file to your phone using Bluetooth. A prompt appears on your phone.
3. Select **View**. A **Security information** prompt appears asking if you want to proceed.
4. Select **Yes**. The **Install software** prompt appears.
5. Select **Install**. The license agreement displays.
6. Carefully read the license agreement, and then click **Yes** if you want to continue installation. A prompt appears, informing you that Mobile Security can only be installed in internal memory.
7. Select **Yes**. The installer extracts the SIS file. When installation is complete, **Mobile Security** appears in your **Applications** menu.

Uninstalling Mobile Security

Mobile Security can be removed using the device's built-in file uninstaller.

To uninstall Mobile Security:

1. On the device, select **Application Controller>Applications**>**Uninstall**.
2. Select **Mobile Security**.
3. Select **Uninstall**. A confirmation prompt appears.
4. Select **Yes**. A prompt appears.
5. Select **Done**.

Chapter 3

Using Mobile Security

This chapter provides an overview of how to navigate the Mobile Security menus and screens.

The topics in this chapter include the following:

Navigating Mobile Security

Navigate through easy-to-use menus to configure Mobile Security settings and to perform tasks.

To perform an action, go to the **Mobile Security** menu, located at the top left of the screens. To configure settings, select the **Edit** menu on the top right of the screens. Select **Done** on individual item screens to return to the next higher level screen. If an action is being performed, halt the action to make the **Done** option available.

Using the Menus

The following table illustrates the series of menus and submenus and the options or tasks associated with each screen.

See your device user's guide for instructions on how to select elements on the screen.

Mobile Security main screen – displays product information and the last successful scan and update
Mobile Security menu– choose a menu item: **Scan**, **Update**, **Virus log**, **Anti-spam log**, **Task log**, **About**, **Quit**
Scan – perform a Manual Scan
Update – update antivirus components
Virus log – view details about viruses Mobile Security detected
Anti-spam log – view details about filtered SMS messages
Task log – view details about tasks such as updates and scans
About – information about Mobile Security
Quit – Exit the Mobile Security interface
Edit menu– choose a menu item: **Scan options**, **Anti-spam options**, **Approved senders list**, **Blocked senders list**
Scan options screen – enable or disable Real-time Scan and Instant Card Scan, and select the layers of compressed files to scan
Anti-spam options screen – enable lists for approved or blocked senders, filter messages from senders without a caller ID, and select whether or not to block a part of a number or whole numbers

Approved senders screen – create, modify, import, and delete a list of senders from whom you want to receive SMS messages
Mobile Security menu– choose a menu item: **Add approved sender**, **Import**, **Delete**
Add approved sender – add an approved sender's name and number
Import – determine the types of senders to import from the contact list in your device
Delete – remove selected sender(s) from the list
Edit – choose **Select all** to perform the same action on all senders in the list
Add – add an approved sender's name and number
Done – return to the **main** screen
Blocked senders screen – create, modify, and delete a list of senders whose SMS messages you want to filter into a spam folder
Mobile Security menu– choose a menu item: **Add blocked sender**, **Delete**
Add blocked sender – add a blocked sender's name and number
Delete – remove selected sender(s) from the list
Edit – choose **Select all** to perform the same action on all senders in the list
Add – add a blocked sender's name and number
Done – return to the **main** screen
Scan – perform a Manual Scan
Update – update antivirus components

Chapter 4

Keeping Antivirus Protection Current

This chapter explains how to help ensure that your device stays protected against the latest virus threats.

The topics in this chapter include the following:

Updating the Antivirus Components

To combat the latest threats, Trend Micro frequently updates the scan engine and virus pattern files used by Mobile Security. When a virus outbreak is occurring, components may be updated several times a day as new variants of a virus are detected. Update your device regularly to help ensure that Mobile Security has the most current antivirus protection. See *Understanding Mobile Security antivirus components* on page 1-3 for more information about the antivirus components.

To perform an update:

1. Establish a GPRS connection with the device.
2. Select **Update** from the main menu. A prompt will appear, asking if you want to continue.
3. Select **Yes**. The **Update** screen appears showing the versions of the Mobile Security program file, scan engine, and virus pattern file. Depending on your system and service provider, a prompt may also appear displaying your account info.
4. If a prompt appears, select **Connect**. Mobile Security begins downloading antivirus components. The task bar shows the progress of the download and installation of the antivirus components.
   - To stop the update, select **Stop**.

Trend Micro strongly recommends performing a Manual Scan to scan for the latest virus threats immediately after updating antivirus components. See Performing a Manual Scan on page 5-4 for instructions.

Chapter 5

Configuring Scan Options

This chapter explains how to configure Mobile Security scan options.

The topics in this chapter include the following:

Scanning for Viruses

Mobile Security can scan all files on your device for viruses. If a file is infected, you have the option to delete it.

Mobile Security provides the following types of scans:

- **Manual Scan** – a user-initiated scan performed on-demand
- **Real-time Scan** – an automatic scan of file operations
- **Instant Card Scan** – an automatic scan of a storage card

Selecting Compressed File Layers to Scan

Mobile Security allows you to select the number of compressed file layers to scan. The maximum ZIP/SIS file levels to scan is 3. Trend Micro recommends selecting this value to ensure that the scan reaches the maximum number of scannable layers.

To select the number of compressed file layers to scan

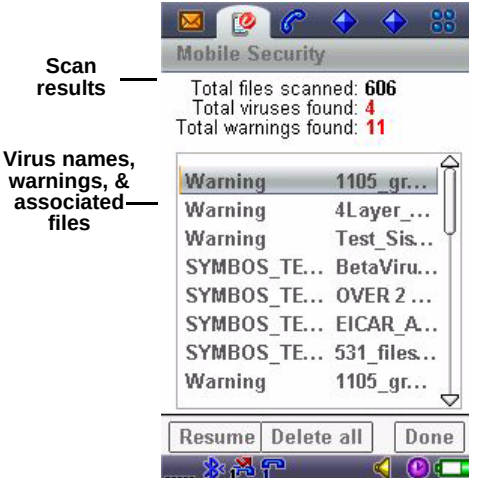
1. From the main menu, select **Edit>Scan options**. The **Scan options** screen appears.
2. Under **ZIP/SIS scan level**, select the number of compressed file layers to scan.
3. Select **Done**.

Performing a Manual Scan

To help ensure your device is protected from viruses, perform a Manual Scan.

To perform a Manual Scan:

- On the Mobile Security main screen, select **Scan**. The Manual Scan screen appears and the scan begins. The number of files scanned, viruses found, and suspicious files found during the last scan displays at the top of the screen. The status bar in the middle of the screen shows the progress of the scan. If Mobile Security detects any viruses or suspicious files, the names of the viruses and files appear at the bottom of the screen. For suspicious files, **Warning** is displayed instead of a virus name
- Select **Stop** at any time during the scan process to pause the scan. Select **Resume** to resume the scan, or **Done** to terminate it.



Trend Micro strongly recommends performing a Manual Scan immediately after transferring new files to your device or downloading new antivirus components (see *Updating the Antivirus Components on page 4-2* *for more information on performing an update).*

Enabling Real-time Scan

You may unknowingly obtain infected programs and compressed files via the Internet or as Email attachments. To help protect your device, enable Real-time Scan (enabled by default). Mobile Security scans executable files when they launch, and all file types when they are opened.

The Mobile Security interface does not need to be open to perform a Real-time Scan.

To enable Real-time Scan:

1. From the main menu, select **Edit>Scan options**. The **Scan options** screen appears.
2. Select the **Enable Real-time Scan** check box.
3. Select **Done**.

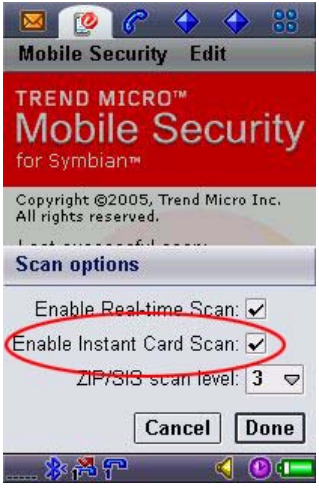
To use Real-time Scan:

- If Mobile Security finds a virus, a prompt appears. Select **Yes** to delete the infected file or **No** to preserve the file.

Do not transfer infected files to another device or to a host PC. Trend Micro strongly recommends deleting all infected files.

Enabling Instant Card Scan

Storage cards also pose a threat to your device if they contain infected files. To perform a scan on storage cards when they are inserted into your device, enable Instant Card Scan (enabled by default).



To enable Instant Card Scan:

1. From the main menu, select **Edit>Scan options**. The **Scan options** screen appears.
2. Select the **Enable Instant Card Scan** check box.
3. Select **Done**.

To perform an Instant Card Scan:

1. Insert a storage card into the device. A prompt displays asking you if you want to scan the card.
2. Select **Yes**.

   The scan begins. The status bar in the middle of the screen shows the progress of the scan. If Mobile Security detects any viruses or suspicious files, the names of the viruses and files appear at the bottom of the screen.

   - Select **Stop** at any time during the scan process to pause the scan. Select **Resume** to resume the scan, or **Done** to terminate it.

Viewing Scan Result Details

Mobile Security saves the names of viruses detected and the names and locations of infected and suspicious files encountered.

To view scan result details:

1. After performing a Manual Scan or Instant Card Scan, select a virus name or warning from the bottom of the screen.
2. The **Details** screen appears.

Unscannable files

Mobile Security is unable to scan some files. If a file is in use by another application, the application may have locked it so it cannot be opened while in use. Also, Mobile Security cannot scan certain compressed (ZIP or SIS) files. The reasons for this include:

- Compression levels exceed the configured scan level (See *Selecting Compressed File Layers to Scan* on page 5-3 for details on setting the compressed file scan level.)
- Extracted size would be too large
- Number of files contained exceeds the maximum file count

These files may be a type of virus known as a file bomb, or they may be harmless. If Mobile Security detects a file of this type, it displays **Warning** on the scan result screen, instead of a virus name. If

Real-time Scan is enabled, Mobile Security will detect any viruses the file contains when they are extracted by an extraction program or the operating system.

Deleting Infected and Suspicious Files

After a Manual Scan or Instant Card Scan, you can delete any infected or suspicious files Mobile Security detects.

To delete infected and suspicious files:

- To delete a single file, select the entry on the scan result screen for the file you want to delete to enter the **Details** screen, and then select **Delete**.
- To delete multiple infected files, select **Delete all**. All infected files will be deleted. Suspicious files will not be deleted.

Do not transfer infected files to another device or to a host PC. Trend Micro strongly recommends deleting all infected files.

Chapter 6

Configuring Anti-spam Options

This chapter explains how to configure Mobile Security Anti-spam options.

The topics in this chapter include the following:

Filtering SMS Spam

To filter unwanted SMS messages, Mobile Security provides the following Anti-spam options:

- **Approved senders list** – configure a list of numbers that Mobile Security allows to send SMS messages to your Inbox
- **Blocked senders list** – configure a list of numbers from which Mobile Security filters SMS messages into a spam folder
- **Filtering messages without caller ID** – have Mobile Security filter SMS messages sent from senders without a registered caller ID into a spam folder

Mobile Security creates a folder in the *Messages* application named `Spam`. To access this folder, open the *Messages* application and select `Spam`.

Access this folder periodically to ensure that Mobile Security did not filter SMS messages you want to receive in your Inbox.

Configuring the Approved Senders List

To receive SMS messages in your Inbox that originate only from a list of trusted senders, enable and configure the approved senders list. This provides the highest level of Anti-spam protection by allowing you to filter all SMS messages from unknown sources.

You can add senders to the approved senders list by importing contacts that already exist in your contact list or by entering their names and phone numbers individually.

Enabling the approved senders list

To enable the approved senders list:

1. From the main menu, select **Edit>Anti-spam options**. The **Anti-spam options** screen appears.
2. Select **Enable approved senders** from the options list.
3. Select **Done**.

Adding approved senders

There are two methods to add senders to the approved senders list:

- Import senders from your contact list
- Manually enter sender details

Importing senders from your contact list

To receive SMS messages in your Inbox from your list of trusted contacts, simply import the contacts from your device into the approved sender's list.

To import senders from your device's contact list:

1. From the main menu, select **Edit>Approved senders list**. The approved senders list screen appears, displaying current entries.
2. Select **Mobile Security>Import**.
3. The **Import options** screen appears.
4. Select the types of contacts to import, if supported on your device.
5. Select the contacts to add. Mobile Security adds the selected contacts to the list of approved senders.
6. Verify that all selected contacts appear on the **Approved senders list** screen.
7. Select **Done**.

Manually entering sender details

To manually enter sender details:

1. From the main menu, select **Edit>Approved senders list**. The approved senders list screen appears, displaying current entries.
2. Select **Add**. The **Add approved sender** screen appears.
3. Type the name and number of the approved sender.
4. Select **Done**. The entry appears in the list.

Modifying approved senders

To modify the details of approved senders:

1. From the main menu, select **Edit>Approved senders list**. The approved senders list screen appears, displaying current entries.
2. Select the entry to modify. The **Edit approved sender** screen appears.
3. Modify the name and number of the approved sender.
4. Select **Done**. The modified entry appears in the list.

Deleting approved senders

To delete senders from the list:

1. From the main menu, select **Edit>Approved senders list**. The approved senders list screen appears, displaying current entries.
2. Select the check box for the entry or entries to delete, or select **Edit>Select all** to delete all entries
3. Select **Mobile Security>Delete**. A confirmation prompt appears.
4. Select **Yes**.
5. Select **Done**.

Configuring the Blocked Senders List

To filter SMS messages into a spam folder that originate only from a list of senders you know distribute spam, enable and configure the blocked senders list.

Enabling the blocked senders list

To enable the blocked senders list:

1. From the main menu, select **Edit>Anti-spam options**. The **Anti-spam options** screen appears.
2. Select **Enable blocked senders** from the options list.
3. Select **Done**.

Adding blocked senders

To add a blocked sender:

1. From the main menu, select **Edit>Blocked senders list**. The blocked senders list screen appears, displaying current entries.
2. Select **Add**. The **Add blocked sender** screen appears.
3. Type the name and number of the blocked sender.
4. Select **Done**. The entry appears in the list.

Modifying blocked senders

To modify the details of blocked senders:

1. From the main menu, select **Edit>Blocked senders list**. The blocked senders list screen appears, displaying current entries.
2. Select the entry to modify. The **Edit blocked sender** screen appears.
3. Modify the name and number of the blocked sender.
4. Select **Done**. The modified entry appears in the list.

Deleting blocked senders

To delete senders from the list:

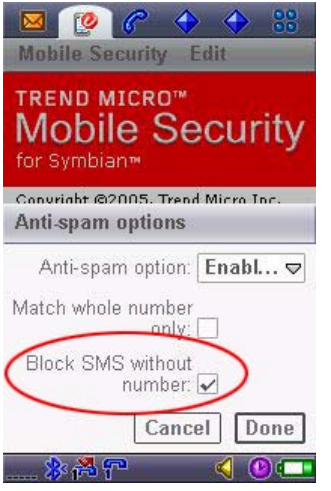
1. From the main menu, select **Edit>Blocked senders list**. The blocked senders list screen appears, displaying current entries.
2. Select the check box for the entry or entries to delete, or select **Edit>Select all** to delete all entries
3. Select **Mobile Security>Delete**. A confirmation prompt appears.
4. Select **Yes**.
5. Select **Done**.

Filtering Messages Without a Caller ID Number

To guard against spam from unknown sources, you can filter SMS messages from any senders that do not register caller ID information.

To filter messages from numbers without a caller ID:

1. From the main menu, select **Edit>Anti-spam options**. The **Anti-spam options** screen appears.
2. Select the **Block SMS without number** check box.
3. Select **Done**.



Blocking SMS messages from senders without a caller ID may filter legitimate messages. Access the spam folder periodically to ensure that Mobile Security did not filter SMS messages you want to receive in your Inbox.

Matching Caller ID Numbers

You can configure Mobile Security to match all or part of a number on the blocked senders list or the approved senders list. Matching only the partial number is primarily useful when your service provider adds area codes or country codes to incoming phone numbers. For example, if you do not select the option to match the entire number and the number "5551234" is in the blocked senders list, Mobile Security blocks messages from any sender whose number contains "5551234". This includes numbers such as 203-555-1234, 555-123-4000, and +1-203-555-1234.

To match the entire number:

1. From the main menu, select **Edit>Anti-spam options**. The **Anti-spam options** screen appears.
2. Select the **Match whole number only** check box.
3. Select **Done**.

Disabling Anti-spam

Disable Anti-spam to receive all SMS messages in your Inbox.

To disable Anti-spam:

1. From the main menu, select **Edit>Anti-spam options**. The **Anti-spam options** screen appears.
2. Select **Disable Anti-spam** from the options list.
3. Select **Done**

Chapter 7

Viewing Logs

This chapter explains the different types of logs available with Mobile Security.

The topics in this chapter include the following:

Viewing Virus Logs

The Virus Log contains details about the viruses and suspicious files detected and the results of the actions Mobile Security took on each virus.

To view the Virus Log:

- From the main screen, select **Mobile Security>Virus log**. The **Virus Log** screen appears displaying a list of detected virus names and dates of detection.

Mobile Security allocates 16KB of memory space for each log type. When this limit is reached, Mobile Security automatically deletes log entries in sequential order starting with the oldest entries.

To view Virus Log entry details:

- Select an entry in the Virus Log. The following information appears:
  - **Date & time** – when Mobile Security detected the virus
  - **Virus name** (infected files only) – the name of the virus
  - **File** – the full path name of the infected file
  - **Warning** (suspicious files only) – information about the virus or potential threat
  - **Action –** the action Mobile Security took on the file. If no action was taken, this field will not appear.
  - **Result –** the result if the action taken. If no action was taken, this field will not appear.

Viewing Anti-spam Logs

The Anti-spam Log contains details such as the date and time of a blocked SMS message, the sender's number, and the result of the action Mobile Security took on the SMS message.

To view the Anti-spam Log:

- From the main menu, select **Mobile Security>Anti-spam log**. The **Anti-spam Log** screen appears displaying the numbers of all blocked messages and the dates Mobile Security blocked them.

To view Anti-spam Log entry details:

- Select an entry in the Anti-spam Log. The following information appears:
  - **Date & time** – when Mobile Security detected the SMS
  - **Caller ID** – the number of the SMS sender
  - **Result** – the action Mobile Security took on the SMS message

Viewing Task Logs

The Task Log contains details such as the task Mobile Security performed (for example, an update or scan), the dates and times of the task, and the result.

To view the Task Log:

- From the main menu, select **Mobile Security>Task log**. The **Task Log** screen appears displaying the tasks and date Mobile Security performed them.

To view Task Log entry details:

- Select an entry in the Task Log. The following information appears:
  - **Start date & time** – when Mobile Security began the action
  - **End date & time** – when Mobile Security completed the action
  - **Task** – the action Mobile Security performed
  - **Result** – the result of the action

Other information relevant to the specific task may also be displayed

Deleting Log Entries

When the number of entries in a log file is too large for the allocated file space, the oldest entries will be deleted. You can also manually delete entries. Clearing all log entries deletes the log file, creating more free storage space on your device.

To delete log entries:

1. From the main screen, select the type of log you want to clear.
   - To delete Virus Log entries, select **Mobile Security>Virus log**.
   - To delete Anti-spam Log entries, select **Mobile Security>Anti-spam log**
   - To delete Task Log entries, select **Mobile Security>Task log**.
2. The appropriate log screen appears.
3. Do one of the following:
   - Select **Clear log**.
   - Select **Mobile Security>Clear log**.
4. A confirmation prompt appears.
5. Select **Yes**.

Chapter 8

Troubleshooting, FAQ, and Technical Support

This chapter provides solutions to common troubleshooting issues, answers to frequently asked questions, and information on how to contact Trend Micro Technical Support.

The topics in this chapter include the following:

Troubleshooting

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

Issue	Recommended Action
The device encountered battery failure while installing Mobile Security and the installation process is not complete	Ensure the device has adequate power and perform the installation process again.
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.
Unable to perform update through a GPRS connection	Confirm your device is connected to the Internet via GPRS connection. If you are connected to a host PC, your device may not allow a GPRS connection. See your device's documentation for details.

Unable to filter SMS messages from senders in the blocked senders list		Your service provider may append additional numbers to incoming calls. If you don't know what numbers your provider will append, clear the **Match whole caller ID only** check box on the **Anti-spam Options** screen (see *Matching Caller ID Numbers* on page 6-11).
Unable to copy a file onto the device		Mobile Security has detected a virus in the file and blocked copying of the file onto your device. To continue the copy operation and risk infecting your device, disable Real-time Scan.

Frequently Asked Questions (FAQ)

- **Can I install Mobile Security on a storage card?**

  No. Mobile Security can only be installed to your device's internal memory.

- **How long can I use Mobile Security and download program and virus pattern file updates?**

  Contact your vendor for licensing details.

- **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 at the same location you installed Mobile Security.

- **How often should I update Mobile Security antivirus components?**

  Trend Micro recommends updating antivirus components on a daily basis.

- **Can Mobile Security scan compressed files?**

  Yes. Mobile Security can scan ZIP and SIS files when they are launched. You can specify up to three layers to scan.

- **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. However, performance may be degraded. Trend Micro recommends you pause the scan until the call is completed, and then resume it. You can view the logs to see details on scans and any viruses Mobile Security found (see *Viewing Logs* on page 7-1).

- **Can I clean infected files?**

  No. Mobile Security gives you the options of deleting or preserving infected files only.

- **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. When the 16KB limit is reached, Mobile Security deletes log entries starting with the oldest.

- **Can I open a file on my device that Mobile Security has identified as being infected?**

  If Real-time Scan is enabled, Mobile Security will block the opening or executing of any infected files it identifies. To perform these operations on an infected file, and risk infecting your device, disable Real-time Scan.

Technical Support

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

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

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

The Trend Micro Security Information Center

Comprehensive security information is available over the Internet, free of charge, on the Trend Micro Security Information Web site:

http://www.trendmicro.com/vinfo/

Visit the Security Information site to:

- Read the Weekly Virus Report, which includes a listing of threats expected to trigger in the current week, and describes the 10 most prevalent threats around the globe for the current week
- View a Virus Map of the top 10 threats around the globe
- Consult the Virus Encyclopedia, a compilation of known threats including risk rating, symptoms of infection, susceptible platforms, damage routine, and instructions on how to remove the threat, as well as information about computer hoaxes

- Download test files from the European Institute of Computer Anti-virus Research (EICAR), to help you test whether your security product is correctly configured
- Read general virus information, such as:
  - The Virus Primer, which helps you understand the difference between viruses, Trojans, worms, and other threats
  - The Trend Micro *Safe Computing Guide*
  - A description of risk ratings to help you understand the damage potential for a threat rated Very Low or Low vs. Medium or High risk
  - A glossary of virus and other security threat terminology
- Download comprehensive industry white papers
- Subscribe to Trend Micro's Virus Alert service, to learn about outbreaks as they happen, and the Weekly Virus Report
- Learn about free virus update tools available to Web masters
- Read about TrendLabs^{SM}, Trend Micro's global antivirus research and support center

Known Issues

Known issues are features in Mobile Security software that may temporarily require a work around. Known issues are typically documented in the Readme document you received with your product. Readme files for Trend Micro products can also be found in the Trend Micro Update Center:

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

Known issues can be found in the Knowledge Base:

http://kb.trendmicro.com/solutions/

Trend Micro recommends that you always check the Readme file for information on known issues that could affect installation or performance, as well as a description of what is new in a particular release, system requirements, and other tips.

Contacting Technical Support

You can contact Trend Micro via fax, phone, 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 PC
- Network type
- Computer and device brand, model, and any additional hardware connected to your device
- Amount of memory and free hard disk space on your device
- Exact text of any error message given

- Steps to reproduce the problem

The Trend Micro Knowledge Base

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 as well as anyone using an evaluation version of a product can access Knowledge Base. Visit:

http://kb.trendmicro.com/solutions/

If you cannot find an answer to a particular question, the Knowledge Base includes an additional service that allows you to submit your question via an email message. Response time is typically 24 hours or less.

Sending Suspicious Files to Trend Micro

You can send your viruses, infected files, Trojans, suspected worms, spyware, and other suspicious files to Trend Micro for evaluation. To do so, visit the Trend Micro Submission Wizard URL:

http://subwiz.trendmicro.com/SubWiz

Select **Submit a suspicious file/undetected virus**. You are prompted to supply the following information:

- **Email –** Your email address where you would like to receive a response from the antivirus team
- **Product –** The product you are currently using. If you are using multiple Trend Micro products, select the product that has the most effect on the problem submitted, or the product that is most commonly in use.
- **Upload File –** Trend Micro recommends that you create a password-protected zip file of the suspicious file, using the word "virus" as the password—then select the protected zip file in the **Upload File** field
- **Description –** Please include a brief description of the symptoms you are experiencing. Our team of virus engineers will "dissect" the file to identify and characterize any threats it may contain and return the cleaned file to you, usually within 48 hours.

Submissions made via the submission wizard/virus doctor are addressed promptly and are not subject to the policies and restrictions set forth as part of the Trend Micro Virus Response Service Level Agreement.

When you select **Next**, an acknowledgement screen displays. This screen also displays a case number for the problem you submitted. Make note of the case number for tracking purposes.

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) TRENDAV, or 877-873-6328

About TrendLabs

TrendLabs[SM] is Trend Micro's global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

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

TrendLabs is staffed by 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 in Tokyo, Manila, Taipei, Munich, Paris, and Irvine, CA, to mitigate virus outbreaks and provide urgent support.

TrendLabs' modern headquarters earned ISO 9002 certification for its quality management procedures in 2000—one of the first antivirus research and support facilities to be so accredited.

Index

R

S

T

U

V

W