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: August, 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

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 security risks, including unsolicited commercial messages (spam) sent by Short Messaging Service (SMS). Version 2.0 of Trend Micro Mobile Security for Symbian extends its protection to possibly harmful messages sent using WAP (Wireless Application Protocol.). It also enables users to quarantine and deny access to security risks, in addition to deleting them.

Understanding viruses and other malware

Malware, short for *malicious software*, is a term used to describe viruses and related threats. However, because viruses were the first and best known type of malware, this entire category of security risks are often referred to as *viruses*. Tens of thousands of viruses and other malware exist.

Although commonly designed to pose security risks to personal computers, viruses and other malicious codes and contents can also attack mobile devices. As people increasingly use mobile devices to share files, check email, and surf the Internet, the risk against security 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 program components

Mobile Security uses the following program components to scan for, identify, and delete detected security risks:

- **Main program:** the Mobile Security main program, which uses the Trend Micro virus pattern file and scan engine to identify security risks and perform actions on detected security risks
- **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 1-4 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. When Mobile Security finds a match, this indicates it has detected a virus.

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 security risks.

Mobile Security Features

Mobile Security includes the following features:

- Manual Scan, Real-time Scan, and Card Scan for viruses and other security risks
- Scan engine and pattern file update (Manual and scheduled)
- Anti-spam (SMS message filtering)
- Protection from harmful WAP(Wireless Application Protocol)-Push messages
- Delete, quarantine and deny access options for handling viruses and other security risks
- Logs for scan results, Anti-spam, harmful WAP-Push messages, and other tasks

Manual Scan, Real-time Scan and 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, executed, received from outside sources, copied, moved, renamed, installed or transferred
- **Card Scan** – automatically scans a storage card when one is detected in your device

Scan engine and virus pattern file update

To ensure that you stay protected against the latest security risks, you must periodically update Mobile Security components. In addition to the normal Update process, you can download updated components to your device via the application's Scheduled Update Settings (See *Keeping Antivirus Protection Current* on page 4-1 for more information).

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.

Logs for scan results, Anti-spam, WAP-Push, and other tasks

Analyze the logs to view details on detected viruses and other security risks, filtered spam messages, WAP-Push messages, program component updates, and all scan results.

What's New in Version 2.0

Mobile Security version 2.0 includes these additional security enhancements and features:

- Quarantine and deny access option for handling security risks
- Protection from harmful WAP-Push messages
- Scheduled update settings

WAP-Push message filtering

WAP-Push is part of the Wireless Application Protocol (WAP) defined by Open Mobile Alliance. WAP-Push messages may be used in the delivery of mobile-related content such as ringtones, news alerts, multimedia messages, incoming email alerts, advertisements and mobile device settings.

With WAP's introduction as another way to deliver multimedia content to mobile devices, spam and security risks may find their way onto mobile devices as WAP-Push messages. WAP-Push messages originate from mobile network operators or some special mobile devices. WAP-Push messages may be misused for sending advertisements, obtaining users' personal or financial information online (and other "phishing" methods), or downloading malicious software packages.

You can filter unwanted WAP-Push messages by enabling WAP-Push Protection on your device. If you frequently receive allowable WAP-Push messages, you can configure a list of phone numbers from which all WAP-Push messages will be allowed. (See *Configuring WAP-Push Protection* on page 7-1 for more information.)

Quarantine and deny access to files

To deal with detected security risks, you can set Mobile Security to quarantine or deny access to files in addition to deleting them. You have to enable real-time scan and set it to quarantine or to deny access to detected security risks as a default action. You can then quarantine or deny access to viruses and other security risks, respectively, the next time they are detected.

When Quarantine is selected , Mobile Security will move the detected security risk to a separate Quarantine List folder. Mobile Security allows you to restore the quarantined file; however, Trend Micro does not recommend this action since it puts your mobile device at risk. (See *Quarantine Detected Security Risks* on page 5-7 for more information.)

When Real-time Scan is set to deny access to detected security risks, these files cannot be executed, opened or copied to another folder. The files stay in their original location. However, the files may be renamed, moved to another location, or deleted. (See *Deny Access to Detected Security Risks* on page 5-9 for more information.)

Scheduled Update settings

Mobile Security allows you to schedule and set the frequency of component updates via Scheduled Update. Once configured, Mobile Security automatically uses these update settings the next time you update the program components. (See *Keeping Antivirus Protection Current* on page 4-1 for more information.)

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 – 1.2MB 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

Trend Micro Mobile Security (TMMS) is a "Symbian Signed" application. Ensure that your mobile phone has a pre-installed "Symbian" root certificate before installing TMMS. To check, from your mobile phone, go to **Applications** > **Control panel** > **Certificate manager** > **Certificate Authority**. Check if **Symbian** is in the **Certificates** list.

Sony Ericsson P800 SmartPhones, launched before the Symbian Signed program was set up, do not have this root certificate pre-installed. Download the `Certification_installation.sis` file (titled "Symbian Signed Certificate for P800") and instructions for installing the certificate from this Web site:

http://developer.sonyericsson.com

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_CNS.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 **Next**. A new prompt appears with language choices.
6. Select the correct language and click **Next**. The license agreement is displayed.
7. 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. Click **Yes**.
8. Click **Finish**. Installation is complete. Mobile Security now appears in your Applications menu.

Bluetooth and Infrared

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

To install via Bluetooth or Infrared:

1. Copy the setup file, `MobileSecurity_UIQ_CNS.sis`, to a Bluetooth/Infrared-enabled PC.
2. Transfer the setup file to your phone using Bluetooth/Infrared. A prompt appears on your phone.

3. Select **View**. Install software prompt appears.
4. Select **Install**. The license agreement is shown.
5. 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.
6. Select **Yes**. The installer extracts the SIS file. When installation is complete, Mobile Security appears in your Applications menu.

Registering Mobile Security

The first time you launch Mobile Security, the **Register** screen is displayed. You may choose to either register immediately or at a later time before the expiration date of the trial version.

To register immediately :

1. From the **Register** screen, type the supplied Activation Code under **AC.**
2. Select **Done**.

To register at a later time (using the trial version):

1. From the **Register** screen, select **Cancel** and then proceed with using the application.
2. Before the product expires, you can go back to **Mobile Security** > **Register** screen, and then register as usual.

At expiration of this product:

- If you are using Trend Micro Mobile Security with a service license, all features will be disabled.
- If you are using Trend Micro Mobile Security with a perpetual license, all features will remain functional but you will not be able to update the program components.

To register after the service license has expired:

1. After launching Mobile Security, the **Register** screen is displayed. From the **Register** screen, type the supplied Activation Code in the **AC** field.
2. Select **Done**.

To register after the perpetual license has expired:

1. From the **Mobile Security** > **Register** screen, type the supplied Activation Code in the **AC** field.
2. Select **Done**.

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 asking you if you would like to keep all configuration and log files.
5. Select **No** (Recommended) to completely remove the files, or **Yes** if you wish to retain the files in your device. Uninstallation is complete.

Chapter 3

Using Mobile Security

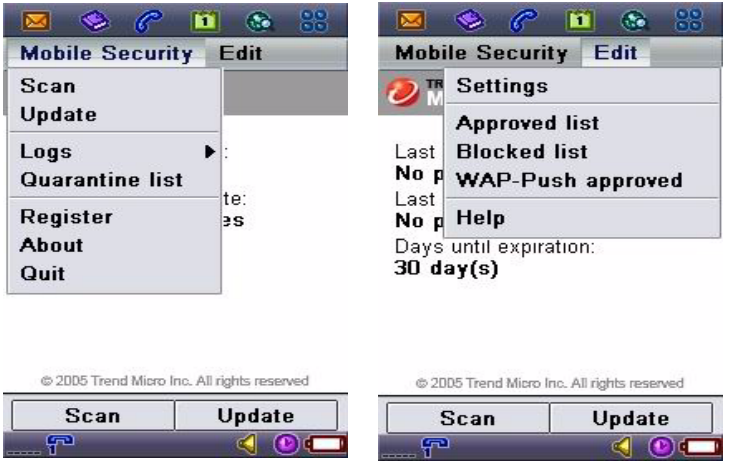
This chapter provides an overview of how to navigate the Mobile Security menus and screens.

The topics in this chapter include the following:

Navigating Mobile Security

To perform an action, go to the **Mobile Security** menu located at top left of the screen, and then click any of the options. To configure settings, choose any of the menu items from the **Edit** option.

For example, choose **Settings** from **Edit**. The options **Scan**, **Anti-spam**, and **Update** are displayed. These options are presented as separate tabs for easy navigation. Scroll to one of the options to view the individual items within the selected option.



Using the Mobile Security and Edit screens

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 expiration and the last successful scan and update
Mobile Security menu– choose a menu item: **Scan, Update, Logs, Quarantine List, Register, About,** and **Quit**
Scan – perform a Manual Scan
Update – update program components
Logs – view details about the viruses, anti-spam, and other tasks such as updates and scans
Quarantine List – display the list of quarantined files
Register – registration details
About – information about Mobile Security
Quit – Exit the Mobile Security interface
Edit items screen – Options inside **Settings (Scan, Anti-spam, Update), Approved List, Blocked List, WAP-Push approved,** and **Help**
Settings – view setting options for scan, anti-spam, and update applications
Scan options screen – select the default action for the Real-time Scan, enable or disable Real-time Scan and Card Scan, and select the layers of compressed files to scan

Anti-spam options screen – enable or disable anti-spam settings, enable WAP-Push Protection and WAP-Push notification
Update options screen – enable scheduled update and frequency
Approved List– view details of SMS approved list
Blocked List– view details of SMS blocked list
WAP-Push approved– view details of WAP-Push approved list
Help – onscreen Help for Mobile Security
Open – open the detailed screen
Edit – modify sender details in the list
Add – add a sender's name and number
Delete – remove selected sender(s) from the list
Select – includes the Select all and Deselect all options
Import – import contact details from mobile device
Done/Back – return to the main screen
Scan – perform a Manual Scan
Update – update program components

Keeping Antivirus Protection Current

This chapter explains how to help ensure that your device stays protected against the latest virus security risks by enabling the Scheduled Update and configuring its settings.

Updating the Program 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 program components* on page 1-3 for more information about the program 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 information.

4. If a prompt appears, select **Connect**. Mobile Security begins downloading program components.The task bar shows the progress of the download and installation of the program components. To stop the update, select **Cancel**.

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

Enabling Scheduled Update

Trend Micro updates the scan engine and pattern file as needed to ensure that you stay protected against the latest security risks. Mobile Security allows you to enable automatic scheduled update and to set the frequency of updates. Once configured, the next time you update the program components, Mobile Security automatically uses these update settings. See *Understanding Mobile Security program components* on page 1-3 for more information about the program components.

Mobile Security allows you to enable automatic scheduled update and to set the frequency of updates. Mobile Security then uses these settings automatically the next time program components are updated.

To enable Scheduled Update:

1. From the main menu, select **Edit > Settings > Update > Scheduled update**. The **Scheduled update** screen appears.
2. Select **Enable** from **Scheduled update** options list.
3. From the **Update frequency** menu, select the frequency in days you wish to regularly check for updates.
4. Select **Done** to return to the main screen.

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 detected, you have the option to either delete or quarantine 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
- **Card Scan** – automatically scans a storage card when one is detected in your device.

Selecting Compressed File Layers to Scan

Scanning compressed file that have been recompressed inside other files, such as a SIS file that contains a ZIP file, requires extra time but provides greater security. You can select the maximum number of compressed SIS or ZIP file layers to scan, up to a maximum of three. 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

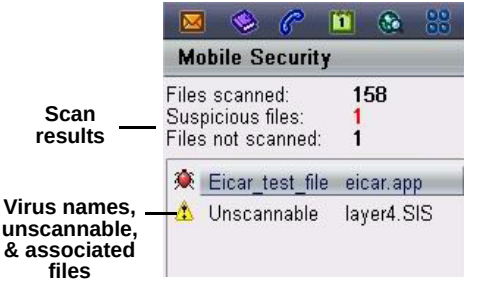
1. From the main menu, select **Edit** > **Settings** > **Scan**. The **Scan** options screen appears.
2. Under **ZIP/SIS scan level**, select the number of compressed file layers to scan.
3. Select **Done**.

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 **Mobile Security** > **Scan**. The Manual Scan screen appears and the scan begins. After scanning, the number of files scanned, viruses found, and other security risks found during the last scan are displayed 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 other security risks, the names of the viruses and files appear at the bottom of the screen. For unscannable files, **Unscannable** is displayed instead of a virus name.

- Select **Pause** at any time during the scan process to pause the scan. Select **Mobile Security** > **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 program components (see Enabling Scheduled Update on page 4-3 for more information on performing an update).

Deleting Detected Security Risks

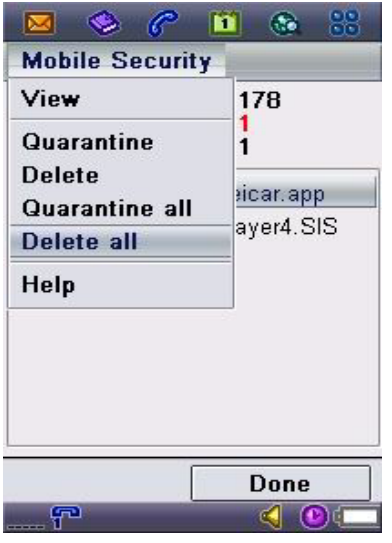
After a Manual Scan, you can delete any detected security risks.

To delete detected security risks:

- 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 **Mobile Security** > **Delete**. Or highlight the entry, and then select **Delete**. Select **Yes** to confirm the deletion.

- To delete all security risks, select **Mobile Security** > **Delete all** . When the confirmation message is displayed, select **Yes**. All detected viruses will be deleted. Unscannable files will not be deleted at this point, but you can delete each file manually following the first procedure for deleting a single file.

Do not transfer detected security risks to another device or to a host PC. Trend Micro strongly recommends deleting all detected security risks.



Quarantine Detected Security Risks

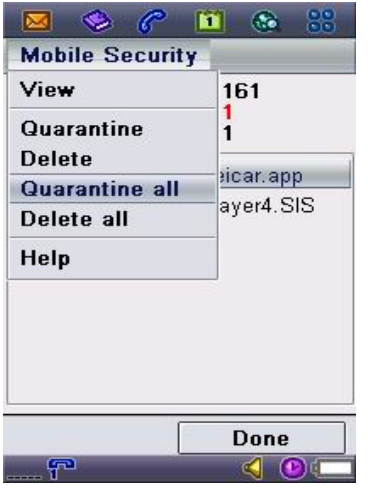
To deal with detected security risks, you can set Mobile Security to quarantine files in addition to deleting them. You can then quarantine files with viruses and other security risks the next time they are detected. When a file is quarantined, its contents will be rewritten and can no longer be executed. To avoid the quarantined files from infecting or damaging your mobile device, Trend Micro encrypts these files.

To automatically quarantine detected security risks:

1. From the **Edit** menu, select **Settings** > **Scan** > **Real-time Scan**. The **Real-time Scan** screen is displayed.
2. Select **Enable** > **Default action**, and then select **Quarantine**.

To quarantine files:

1. To quarantine all viruses and other malware, from the scan result screen, select **Mobile Security** > **Quarantine all**. Unscannable files will not be quarantined.
2. To quarantine a detected security risk, select the file you want to quarantine from the scan result individually, and then select **Mobile Security** > **Quarantine**. A confirmation message is displayed.
3. Select **Yes**, and then select **Done**.



Mobile Security allows you to restore the quarantined file; however, Trend Micro does not recommend this action since it puts your mobile device at risk.

To restore quarantined files

1. From the main menu, select **Mobile Security** > **Quarantine List**. Select the file you want to restore from the **Quarantine List**.
2. Select **Mobile Security** > **Restore**. The confirmation message is displayed.
3. Select **Yes**. The quarantined file is restored.

Deny Access to Detected Security Risks

When Real-time Scan is set to deny access to detected security risks, these files cannot be executed, opened or copied to another folder. The files stay in their original location. However, the files may be renamed or deleted.

To automatically deny access to detected security risks:

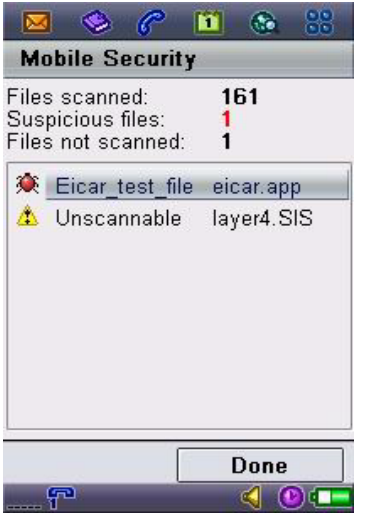
1. From the **Edit** menu, select **Settings** > **Scan** > **Real-time Scan**. The **Real-time Scan** screen is displayed.
2. Select **Enable** > **Default action**, and then select **Deny access**.

Viewing Scan Result Details

Mobile Security saves the names and locations of detected viruses and other security risks.

To view scan result details:

1. After performing a Manual Scan , select a virus name or an unscannable file from 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.)
- Compressed files with password
- 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 **Unscannable** 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.

Enabling Real-time Scan

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

You may unknowingly obtain security risks via the Internet or as email attachments. To help protect your device, enable Real-time Scan (enabled by default). Mobile Security then scans files whenever they are opened, executed, received from outside sources, copied, moved, renamed, installed or transferred. If Mobile Security finds a virus or a security risk, a prompt appears along with the optional audio alert. For unscannable files, the files are recorded onto the scan log.

To enable Real-time Scan:

1. From the main menu, select **Edit > Settings > Scan**. The **Scan** options screen appears.
2. From the Real-time Scan option, select the **Enable Real-time Scan** check box. The **Default action** option is displayed.
3. Select a default action for real-time scan and the ZIP/SIS scan level.
4. Select **Done** to return to the main screen.

.

Do not transfer detected security risks to another device or to a host PC. Trend Micro strongly recommends deleting all detected security risks.

Enabling Card Scan

To enable Card Scan:

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

To perform a 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 security risk, the names of the security risks and files appear at the bottom of the screen.
3. Select **Pause** at any time during the scan process to pause the scan. Select **Resume** to resume the scan, or **Done** to terminate it.

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

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** > **Settings** > **Anti-spam**. The **Anti-spam** options screen appears.
2. Select **Use approved list** 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 list**. The **Approved list** screen appears, displaying current entries.
2. Select **Mobile Security > Import**.
3. The mobile phone's Contacts List screen appears.
4. Select the types of contacts to import, if supported on your device.
5. Select the contacts to add, and then select **Done**. Mobile Security adds the selected contacts to the list of approved senders.

6. Verify that all selected contacts appear on the **Approved list** screen.
7. Select **Back** to return to the main screen.

Manually entering sender details

To manually enter sender details:

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

Modifying approved senders

To modify the details of approved senders:

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

Deleting approved senders

To delete senders from the list:

1. From the main menu, select **Edit > Approved list**. The **Approved list** screen appears, displaying current entries.
2. To delete one contact, scroll to the contact information, and then select **Delete**. When the confirmation prompt appears, select **OK**.
3. To delete all contacts, select **Mobile Security> Select all**.
4. Select **Mobile Security > Delete**. When the confirmation prompt appears, select **Yes**.
5. Select **Back** to return to the main screen.

Configuring the Blocked Senders List

Enable the blocked list to filter SMS messages that originate only from a list of senders that you know distribute spam. Mobile Security allows you to configure the blocked list by importing senders from your contact list or by manually entering sender details. You can then modify or later delete these entries.

Enabling the blocked list

To enable the blocked list:

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

Using the blocked list

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

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

Importing senders from your contact list

To block SMS messages that are sent from numbers on your contact list, import the desired contacts into the **Blocked list**.

To import senders from your device's contact list:

1. From the main menu, select **Edit** > **Blocked list**. The **Blocked list** screen appears, displaying current entries.
2. Select **Mobile Security** > **Import**.
3. The mobile phone's Contacts List screen appears.
4. Select the types of contacts to import, if supported on your device.
5. Select the contacts to add, and then select **Done**. Mobile Security adds the selected contacts to the list of blocked senders.
6. Verify that all selected contacts appear on the **Blocked list** screen.
7. Select **Back** to return to the main screen.

Manually entering sender details

To manually enter sender details:

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

Modifying blocked senders

To modify the details of blocked senders:

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

Deleting blocked senders

To delete blocked senders from the list:

1. From the main menu, select **Edit > Blocked list**. The **Blocked list** screen appears, displaying current entries.
2. To delete one contact, scroll to the contact information, and then select **Delete**. When the confirmation prompt appears, select **OK**.
3. To delete all contacts, select **Mobile Security> Select all**.
4. Select **Mobile Security > Delete**. When the confirmation prompt appears, select **Yes**.
5. Select **Back** to return to the main screen.

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** > **Settings** > **Anti-spam**. The **Anti-spam options** screen appears.
2. Select **Disable Anti-spam** from the options list.
3. Select **Done**.

Chapter 7

Configuring WAP-Push Protection

This chapter explains how WAP Push Protection is configured in Mobile Security.

The topics in this chapter include the following:

Enabling WAP-Push Protection

WAP-Push is part of the Wireless Application Protocol (WAP) defined by Open Mobile Alliance. WAP-Push messages may be used in the delivery of mobile-related content such as ringtones, news alerts, multimedia messages, incoming email alerts, advertisements and mobile device settings.

With WAP's introduction as another way to deliver multimedia content to mobile devices, spam and security risks may find their way onto mobile devices as WAP-Push messages. WAP-Push messages originate from mobile network operators or some special mobile devices. WAP-Push messages may be misused for sending advertisements, obtaining users' personal or financial information online (and other "phishing" methods), or downloading malicious software packages. All this can leave the mobile device vulnerable to harmful or malicious WAP-Push messages.

You can filter unwanted WAP-Push messages by enabling WAP-Push Protection on your device. If you frequently receive spam from the same numbers, you can configure a list of phone numbers from which all WAP-Push messages are allowed. This provides the highest level of protection by allowing you to filter all WAP-Push messages from unknown sources.

You can add senders to the approved senders list by entering their names and phone numbers individually.

To enable WAP-Push Protection:

1. From the main menu, select **Edit > Settings > Anti-spam**. The **Anti-spam settings** screen appears.
2. Select **Enable** from the **WAP-Push protection** options list.
3. Select **Done** to return to the main screen.

Adding WAP-Push approved senders

To receive WAP-Push messages on your browser, you can manually add senders to the WAP-Push approved list. When using the approved senders list, Mobile Security will prompt you to confirm receipt of all other senders.

To manually enter sender details:

1. From the main menu, select **Edit > WAP-Push approved**. The **WAP-Push approved list** screen appears, displaying current entries.
2. Select **Mobile Security** > **Add**.
3. Type the name and number of the approved sender.
4. Select **Done** to confirm that the new entry appears in the list.

Modifying WAP-Push approved senders

To modify the details of approved senders:

1. From the main menu, select **Edit > WAP-Push approved**. The **WAP-Push approved list** screen appears, displaying current entries.
2. Select the entry to modify, and then click **Mobile Security** > **Edit**.
3. Modify the name and number of the approved sender.

4. Select **Done** to confirm that the modified entry appears in the list.

Deleting WAP-Push approved senders

To delete senders from the list:

1. From the main menu, select **Edit > WAP-Push approved**. The **WAP-Push approved list** screen appears, displaying current entries.
2. To delete one contact, scroll to the contact information, and then select **Delete**. When the confirmation prompt appears, select **OK**.
3. To delete all contacts, select **Mobile Security> Select all**.
4. Select **Mobile Security > Delete**. When the confirmation prompt appears, select **Yes**.
5. Select **Back** to return to the main screen.

Chapter 8

Viewing Logs

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

The topics in this chapter include the following:

Viewing the Scan Log

The Scan Log contains details about the viruses and security risks detected and the results of the actions Mobile Security took on each virus.

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 the Scan Log:

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

To view Scan Log entry details:

- Select an entry in the Scan Log. The following information appears:
  - **Date & time –** when Mobile Security detected the virus
  - **Risk name –** the name of the virus or other malware. For unscannable files, **Details** is displayed.
  - **File –** the full path name of the detected security risk
  - **Details –** information about the detected security risk

- **Action –** the action Mobile Security took on the file. If no action was taken, this field will not appear.
- **Result –** the result of the action taken. If no action was taken, this field will not appear.

Viewing the Anti-spam Log

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

To view the Anti-spam Log:

- From the main menu, select **Mobile Security > Logs > 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 and WAP-Push mesages
  - **Caller ID** – the number of the message sender
  - **Type** – the type of message (e.g., SMS, WAP-Push)
  - **Result** – the action Mobile Security took on the SMS or WAP-Push message

Viewing the Task Log

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 > Logs > Task log**. The **Task Log** screen appears displaying the tasks and date Mobile Security performed them.

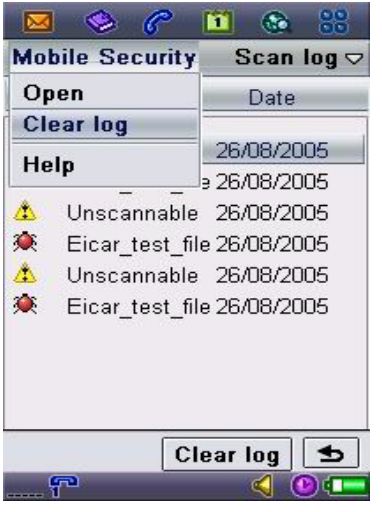
To view Task Log entry details:

- Select an entry in the Task Log. The following information appears:
  - **Start date** – when Mobile Security began the action
  - **End date** – when Mobile Security completed the action
  - **Task** – the action Mobile Security performed
  - **Files scanned** – the number of scanned files
  - **Files not scanned** – the number of unscanned files
  - **Suspicious files** – the number of suspicious files
  - **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.



To delete log entries:

1. From the main screen, select the type of log you want to clear.
   - To delete Scan Log entries, select **Mobile Security > Logs > Scan log**.
   - To delete Anti-spam Log entries, select **Mobile Security > Logs > Anti-spam log**
   - To delete Task Log entries, select **Mobile Security > Logs > Task log**.
2. The appropriate log screen appears.
3. Select **Clear log**.
4. A confirmation prompt appears.
5. Select **OK**.
6. Click **Back** to return to the main screen.

Chapter 9

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 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 program components?**

  Trend Micro recommends updating program 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 .

- **Can I clean detected security risks?**

  No. Mobile Security only gives you the options of deleting, placing in quarantine or denying access to detected security risks.

- **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 detected?**

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

- **Can Mobile Security work correctly if I have installed another antivirus product on the same phone?**

  Trend Micro recommends that you remove all other antivirus software in your mobile device before installing Mobile Security. The existence of other antivirus products may interfere with some of Trend Micro Mobile Security's functions.

- **Where are the quarantined files located?**

  To avoid the quarantined files from infecting or damaging your mobile device, Trend Micro encrypts these files. From the main menu, select **Options** > **Quarantine List**. You can then restore the quarantined files; however, Trend Micro does not recommend this action.

- **How can I see my blocked SMS messages?**

The blocked SMS messages are placed in a folder named **Spam** under the **Message** menu. You can read these messages, reply to them, or restore them to the SMS folder. These blocked SMS messages occupy storage space so it helps to clear them for a period of time.

Technical Support

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

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

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 security risks expected to trigger in the current week, and describes the 10 most prevalent security risks around the globe for the current week
- View a Virus Map of the top 10 security risks around the globe
- Consult the Virus Encyclopedia, a compilation of known security risks 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 security risks
  - 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™, 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 security risks to Trend Micro

You can send your viruses, detected security risks, Trojans, suspected worms, spyware, and other security risks 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 security risks it may contain and return the cleaned file to you, usually within 48 hours.

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.**

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.

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

About TrendLabs

TrendLabs™ 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 security risks. 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 worldwide to mitigate virus and other security risk 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