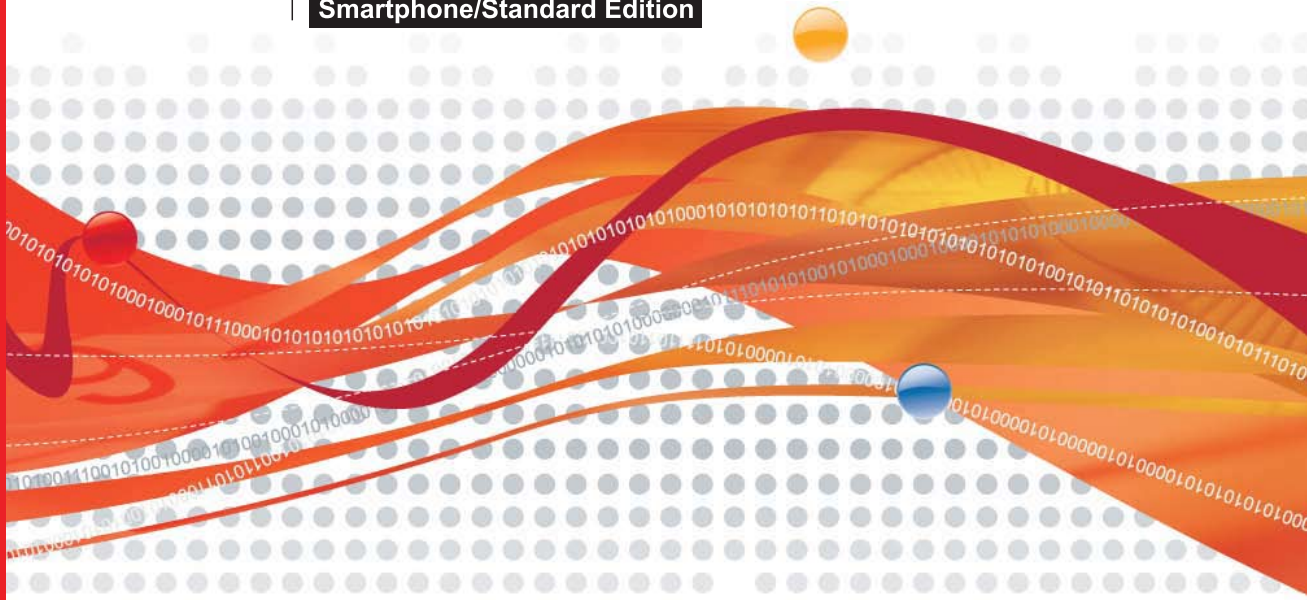
Trend Micro™ Mobile Security 3

for Microsoft™ Windows Mobile™ 5/6

Smartphone/Standard Edition



User's Guide

Release Date: September, 2007

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

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

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

Contents

Chapter 1

Introducing Trend Micro™ Mobile Security

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

This chapter covers the following topics:

Mobile Security Overview

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

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

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

Understanding Mobile Threats

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

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

Protecting Your Handheld Device

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

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

Mobile Security Features

Mobile Security offers the following features:

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

Antivirus scanning

Mobile Security incorporates award-winning Trend Micro antivirus technology to detect viruses and other malware on your handheld device. Mobile Security is especially designed to scan for mobile viruses and other malware and allows you to quarantine or delete detected files.

Regular component updates

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

Firewall

Trend Micro Mobile Security 3.0 includes the Trend Micro firewall module, which several award-winning Trend Micro products incorporate. With the firewall, you can use predefined security levels to filter network traffic. You can also define your own filtering rules and filter network traffic from specific IP addresses and on specific ports. The intrusion detection system (IDS) allows you to block attempts to continually send multiple packets to your device. Such attempts typically constitute a denial of service (DoS) attack and can render your device too busy to accept other connections.

SMS Anti-spam

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

WAP Push protection

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

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

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

Event logs

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

Chapter 2

Installing Trend Micro Mobile Security

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

This chapter covers the following topics:

System Requirements

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

Handheld device

Ensure that your handheld device meets the following requirements:

- **Operating system**—Windows Mobile™ 5.0/6.0 - Smartphone/Standard
- **Storage space**—3MB minimum free space
- **Memory—**2MB minimum free memory; 3MB recommended

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

Determining your device platform

To determine the Windows Mobile version running on your device:

1. Select **Start > Settings > More...**.
2. Select **About**.
3. On the **About** screen (see Figure 2-1), verify the Windows Mobile version.

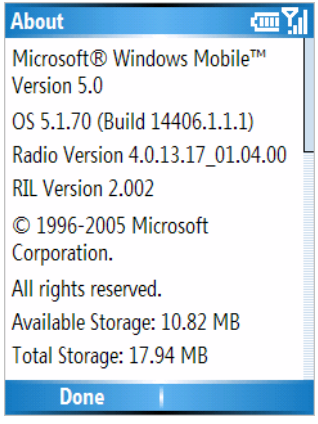


Figure 2-1. Windows Mobile About screen

Host computer

Installing Mobile Security does not require a host computer, but you may need to connect the device to a computer for the following reasons:

- To copy the installation file to your handheld device
- To update the product's antivirus components through the computer's Internet connection

For these purposes, you need a Microsoft™ Windows™-based computer running ActiveSync™ 4.1 or later.

Before Installing

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

Getting the latest version

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

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

Obtaining a license

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

To purchase a new license, visit:

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

Using ActiveSync

You may need to use Microsoft ActiveSync to connect your mobile device to a host computer before you can install Mobile Security. You can download updates for Mobile Security when you connect to a computer with an active Internet connection.

To copy or run the installation file from a computer, connect the device to the computer as a guest. However, you need a *standard synchronization relationship* between the device and the computer to update Mobile Security through the computer's Internet connection. See your ActiveSync documentation for more information.

To get updates using the computer's Internet connection, ensure that the device's proxy server settings match the Internet Explorer proxy settings on the computer. ActiveSync should be able to do this automatically, but may fail if Internet Explorer uses a script to define proxy server settings. When necessary, consult your service provider or your network administrator for the correct proxy server settings and manually configure your device.

Table 2-1 shows the required ActiveSync settings for common tasks.

Task	Required ActiveSync Settings
Copy installer file	Connected as a guest
Update components	Standard synchronization relationship; same proxy server settings on device and computer

TABLE 2-1. Required ActiveSync settings

ActiveSync displays the name of the device and automatically synchronizes data when in a standard synchronization relationship as shown in Figure 2-2.

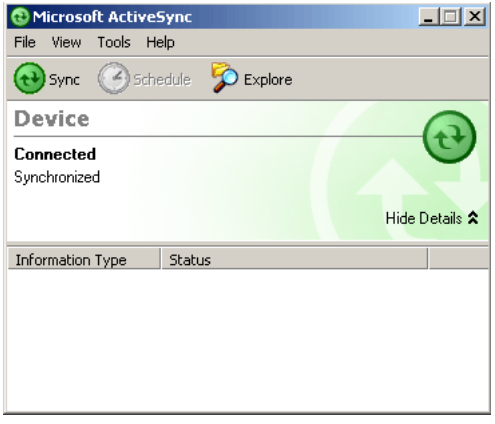


FIGURE 2-2. Microsoft ActiveSync connected in a standard synchronization relationship

ActiveSync displays the word "Guest", as shown in Figure 2-3, when your device is connected as a guest.

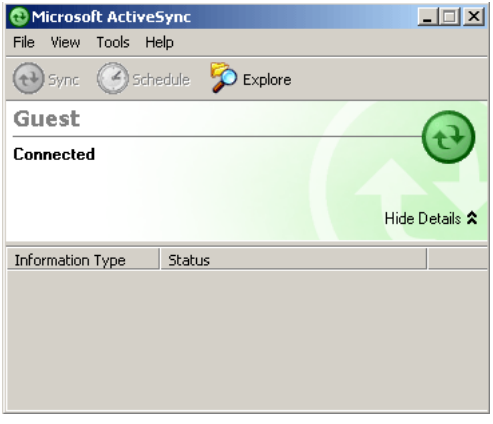


FIGURE 2-3. Microsoft ActiveSync with device connected as a guest

For more information on ActiveSync synchronization relationships, refer to the Microsoft ActiveSync help topic Overview of synchronization relationships.

Installation

To install Mobile Security, you need the CAB installation file `MobileSecurity_SP.cab`.

To install Mobile Security:

1. Copy the CAB installation file to your handheld device. You may need to use ActiveSync to connect your device to a host computer. You can also use a memory card to transfer the file.
2. On your device, use File Explorer to navigate to the location of the CAB file.
3. Open the CAB file to begin installation.
4. Select **Accept** if you accept the terms of the license agreement. The CAB file extracts and installs Mobile Security.
5. If installation is successful, Mobile Security will launch and prompt you for your Activation Code. You can provide the Activation Code to register the product or use the product with a trial license for thirty days.

On some devices, Mobile Security may require a restart to load the firewall or the WAP Push protection driver.

Registration

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

To register Mobile Security:

1. On the main screen select **Menu** > **Register**. The registration screen opens as shown in Figure 2-4.
2. Type the Activation Code, then select **Activate**.

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

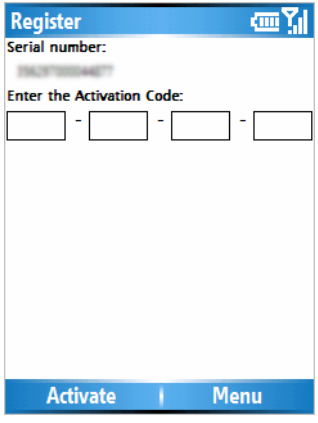


Figure 2-4. Register screen

Uninstallation

To uninstall Mobile Security, use either of two methods:

- Directly on the device
- Through a host computer

To uninstall directly on the device:

1. On the device, select **Settings** > **Remove Programs**.
2. Select **Trend Micro Mobile Security**.
3. Press the action key or select **Menu > Remove**.
4. When Windows Mobile prompts you for confirmation, select **Yes**.
5. When Mobile Security prompts you to save settings, select either of the following:
   - **Yes** to save your current settings, including firewall rules and anti-spam lists, so you can use them when you reinstall Mobile Security.
   - **No** to delete your current settings.

To uninstall through a host computer:

1. Connect the device to a host computer.
2. Open Microsoft ActiveSync on the host computer.
3. On the ActiveSync panel, click **Tools** > **Add/Remove Programs**.
4. In the programs list, select **Trend Micro Mobile Security** and click **Remove**.
5. When ActiveSync prompts for your confirmation, click **OK**.
6. When Mobile Security prompts you to save settings, select either of the following:
   - **Yes** to save your current settings, including firewall rules and anti-spam lists, so you can use them when you reinstall Mobile Security.
   - **No** to delete your current settings.

Chapter 3

Getting Started with Trend Micro Mobile Security

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

This chapter covers the following topics:

Updating Antivirus Components

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

To update Mobile Security:

1. Ensure that you are connected to the Internet.
2. Select **Update** from the main screen. The **Update** screen shows the component versions. The bar shows the status of the update. To cancel the update, select **Cancel**.

For more information on updating the product, see Updating Antivirus Components on page 4-1.

Scanning for Viruses

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

For more information on Mobile Security antivirus capabilities, see Scanning for Viruses on page 5-1.

Understanding the Interface

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

- Main screen
- Menu items

Main screen

Mobile Security opens with its main screen (see Figure 3-1). The following actions are available on the main screen:

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

TABLE 3-1. Main screen interface items

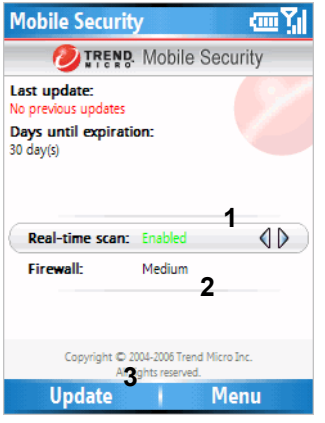


Figure 3-1. Main screen

Menu items

The main screen menu (see Figure 3-2) lets you access all product features. The main screen menu items and the actions they perform are:

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

TABLE 3-2. Main screen menu items

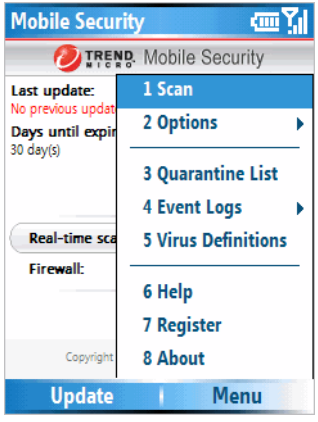


Figure 3-2. Main screen menu

Reviewing Default Protection Settings

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

Feature	Default Setting	Resulting Action
Real-time scanner	Enabled	Product scans files that are being accessed.
Real-time action	Quarantine	Product encrypts and moves detected files.
Card scan	Disabled	Product does not scan memory cards automatically when inserted.
File types to scan	All	Product scans all files for viruses and other malware.
CAB/ZIP layers to scan	3 (maximum)	Product extracts compressed files (CAB/ZIP) to up to three compression layers before scanning them for viruses. If a file is compressed in more than three layers, product considers the file unscannable.
Wireless connection alert	Enabled	Product displays a confirmation message before opening a GPRS or other wireless connections to access the Internet.

TABLE 3-3. Default protection settings

Feature	Default Setting	Resulting Action
Automatic updates	Enabled	Product automatically checks for, downloads, and installs updates.
Update frequency	8 hours	Product attempts to check for updates 8 hours after the last update check.
Force update after	30 days	Product runs an update every 30 days, opening a wireless connection when necessary. This update will run every 30 days, regardless of whether other updates have run.
Firewall	Enabled	Product filters incoming and outgoing network traffic. See *Firewall rules* on page 6-5 for information on default firewall rules.
Intrusion detection system (IDS)	Enabled	Product protects against denial of services attacks.

TABLE 3-3. Default protection settings (continued)

Feature	Default Setting	Resulting Action
Firewall protection level	Medium	Firewall allows all outgoing traffic and blocks all incoming traffic. Note that Mobile Security includes predefined firewall rules, which take precedence over the selected protection level.
SMS anti-spam	Disabled	Product does not filter SMS messages and allows all messages to reach the message inbox.
WAP Push protection	Disabled	Product does not filter WAP Push messages and allows all messages to reach the device.

TABLE 3-3. Default protection settings (continued)

Chapter 4

Updating Antivirus Components

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

This chapter covers the following topics:

Connecting to ActiveUpdate Servers

To update Trend Micro Mobile Security, you must connect to Trend Micro ActiveUpdate servers through the Internet. Consult your device documentation and your service administrator for instructions on connecting your device to the Internet.

Updating Program Components

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

Type	Description
Manual	User-initiated; you can run these updates anytime.
Automatic	Run at specified intervals from the last update check; this update only runs when your device is connected to the Internet.
Forced	Run at specified intervals regardless of whether other updates have been run within the interval period; forced updates will open the default wireless connection if your device is not connected to the Internet.

TABLE 4-1. Update types

Automatic updates

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

To configure automatic update intervals:

1. Select **Menu > Options > Update Options**. The **Update Options** screen opens as shown in Figure 4-1.
2. On the **Update Options** screen, ensure that **Enable automatic updates** is selected.
3. Select your preferred **Update frequency**. Mobile Security will check for updates at this interval, counting from your last update check. This update will run only if your device is connected to the Internet.

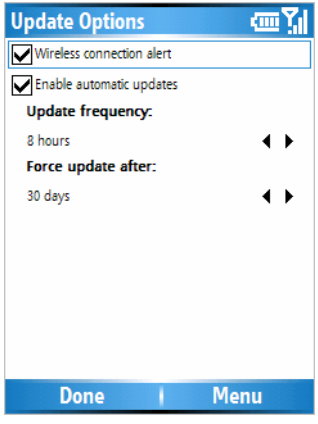


Figure 4-1. Update Options screen

4. Select an interval for forced updates under **Force update after**. Mobile Security will open your default Internet connection and check for updates at this interval, regardless of whether other updates have been run.
5. Select **Done**.

*Mobile Security may open a GPRS, CDMA2000, or other wireless connections during forced updates. If you want to Mobile Security to display a message (shown in Figure 4-2) before opening a wireless connection, select **Wireless connection alert**.*

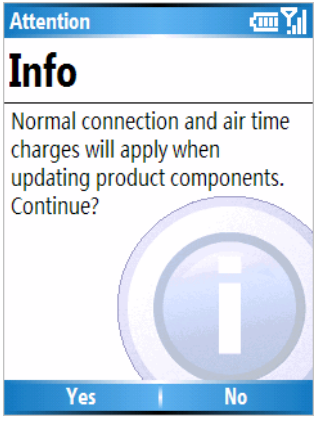


Figure 4-2. Wireless connection alert message

Manual updates

To perform a manual update:

1. Ensure that you are connected to the Internet.
2. Select **Update** from the main menu. The **Update** screen shows the component versions. The bar shows the status of the update. To cancel the update, select **Cancel**.

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

Chapter 5

Scanning for Viruses

Trend Micro Mobile Security scans your device for mobile viruses and other malware. Read this chapter to understand the antivirus features of Mobile Security.

This chapter covers the following topics:

Antivirus Scan Types

Mobile Security offers the following antivirus scan types:

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

TABLE 5-1. Antivirus scan types

Manual Scan

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

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

Real-time Scan

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

Enabling real-time scan

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

To enable real-time scan:

1. Select **Menu > Options > Scan Options** on the main screen. The Scan Options screen opens as shown in Figure 5-1.
2. Select **Enable real-time scan**.
3. Select **Done**.

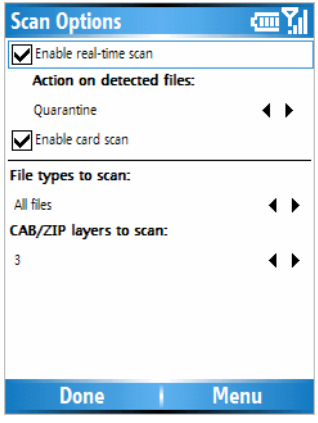


Figure 5-1. Scan Options screen

*To disable the real-time scanner, clear **Enable real-time scan** in the **Scan Options** screen. If you disable the real-time scanner, your device will be unprotected against viruses and other malware.*

Setting the action on detected files

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

Select your preferred real-time action under **Action on detected files** on the **Scan Options** screen.

Card Scan

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

To enable card scan:

1. Select **Menu > Options > Scan Options** on the main screen.
2. Select **Enable card scan**.
3. Select **Done**.

Scan Results

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

Viewing scan results

After a manual or card scan, Mobile Security displays a list of detected and unscannable files as shown in Figure 5-2. You can either quarantine or delete these files.

Scan result items can either be detected files or unscannable files as explained in Table 5-2.

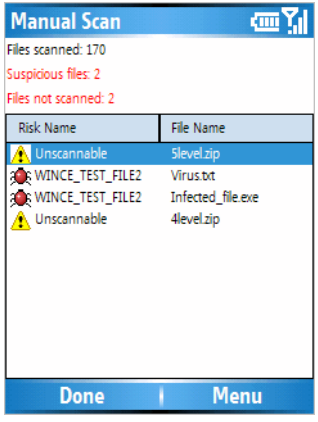


Figure 5-2. Scan results screen

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

TABLE 5-2. Scan result items

To view details on a detected or unscannable file, select the file and press the action button.

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

Handling detected or unscannable files

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

To delete or quarantine detected or unscannable files:

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

*To quarantine or delete all detected or unscannable files, select **Delete All** or **Quarantine All**.*

Quarantined Files

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

To open the list, select **Menu > Quarantine List** on the main screen. Figure 5-3 shows the **Quarantine List** screen.

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

To restore files from quarantine:

1. On the **Quarantined List** screen, select the file you wish to restore.
2. Select **Menu > Restore**.

Do not open detected files after restoring them.

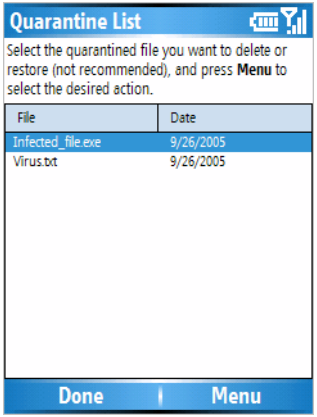


Figure 5-3. Quarantine List screen

Advanced Antivirus Settings

You can select which types of files to scan. For compressed files, you can specify the maximum number of compression layers (up to three) that Mobile Security will support before considering compressed files unscannable.

File types to scan

Mobile Security can scan all files, executable and compressed files, or executable files only.

Option	Description
All files	Every file on the device, except operating system files stored in read-only memory (ROM)
Executable and Zip/Cab files	Files with `.EXE` and `.DLL` extensions and compressed files in `.ZIP` and `.CAB` formats; `.CAB` files are commonly used to install applications
Only executable files	Files with `.EXE` and `.DLL` extensions

TABLE 5-3. Options for file types to scan

Compression layers to scan

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

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

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

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

Configuring advanced scan settings

Configure the advanced scan settings, such as the files types and the compression layers to scan, in the **Scan Options** screen.

To configure advanced scan settings:

1. From the main menu, select **Menu > Options > Scan Options**.
2. Under **File types to scan**, select the types of files to scan for viruses. For more information on the file type options, see Table 5-3.
3. If you selected **All files** or **Executable and CAB/ZIP files**, select the number of CAB and ZIP file layers to scan under **CAB/ZIP layers to scan** option.
4. Select **Done**.

*The item **Action for detected files** applies only to the real-time scan. See Setting the action on detected files on page 5-4.*

Information on Mobile Viruses

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

To view additional details on a virus, select the virus and select **View**.

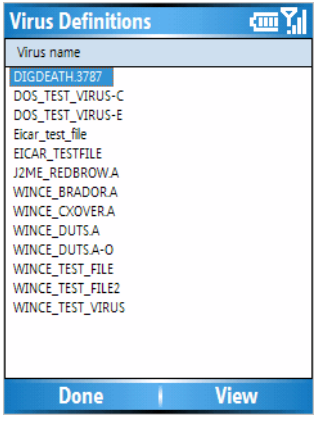


Figure 5-4. Virus Definitions screen

Using the Firewall

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

This chapter covers the following topics:

Understanding Firewalls

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

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

Ports are typically associated with certain applications and services.
See Firewall rules on page 6-5 for more information.

Understanding Mobile Security Firewall Filtering

Mobile Security provide two filtering methods with the firewall:

- Predefined protection levels
- Firewall rules

In addition to the predefined protection levels and the firewall rules, Mobile Security implements firewall policies in the background to ensure that basic network communication, ActiveSync communication, and component updates are not affected.

Predefined protection levels

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

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

TABLE 6-1. Predefined protection levels

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

Firewall rules

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

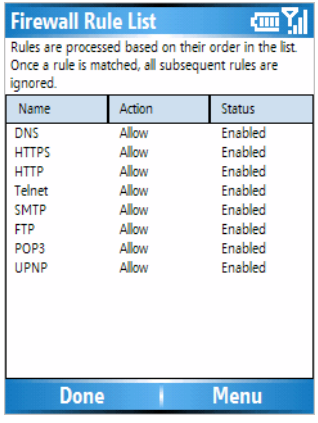


Figure 6-1. Firewall Rule List screen

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

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

TABLE 6-2. Default firewall rules

You can modify the default firewall rules and create your own rules. For more information, see *Advanced Firewall Settings* on page 6-8.

Enabling the Firewall

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

To enable the firewall:

1. Select **Menu > Options > Firewall Options** on the main screen. The **Firewall Options** screen opens as shown in Figure 6-2.
2. Select **Enable firewall**.
3. Select **Done**.

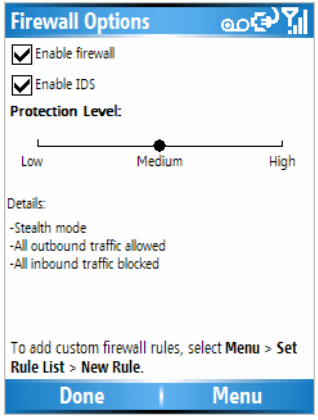


Figure 6-2. Firewall Options screen

Configuring the Firewall Protection Level

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

For details on the predefined protection levels, see Predefined protection levels on page 6-4.

To configure your firewall protection level:

1. Select **Menu > Options > Firewall Options** on the main screen.
2. Ensure that **Enable firewall** is selected.
3. Under **Protection level**, select your preferred protection level.
4. Select **Done**.

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

Advanced Firewall Settings

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

Creating firewall rules

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

To create a firewall rule:

1. Select **Menu > Options > Firewall Options** on the main screen.
2. Ensure that **Enable firewall** is selected.
3. Select **Menu > Set Rule List**. The **Firewall Rule List** screen opens.
4. Select **Menu > New Rule**. The **Rule Details** screen opens as shown in Figure 6-3.

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

5. Provide a unique name for the rule.

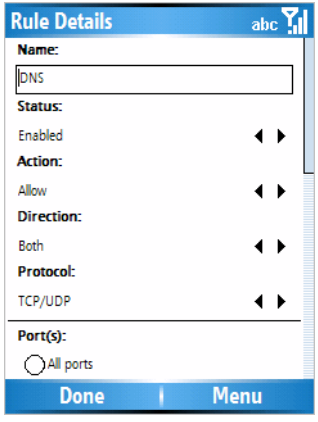


Figure 6-3. Rule Details screen

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

Item	Options	Definition
Status	• Enabled • Disabled	Turns the rule on or off
Action	• Deny • Allow • Log only	Determines whether a connection attempt that matches the rule will be allowed, denied, or only logged
Direction	• Inbound • Outbound • Both	Determines whether this rule applies to incoming or outgoing connections or both
Protocol	• All • TCP/UDP • TCP • UDP • ICMP	Determines the network protocol to which this rule applies

TABLE 6-3. Rule details screen items

Item	Options	Definition
Port(s)	• All ports • Port range • Specific ports	Determines the ports in the device (for incoming connections) or remote system (for outgoing connections) where access is allowed or denied; you can allow or deny access to all network ports, a port range, or up to 32 specific ports When specifying ports, separate each port with a comma. **Note:** When the ICMP is selected under **Protocol**, you cannot specify ports.
IP address(es)	• All IP addresses • Single IP address • IP address range • Subnet	Determines the IP addresses to which access is allowed or denied; you can allow or deny access to all IP addresses, a specific IP address, an IP address range, or a subnet **Note:** To apply the rule to a subnet, you must specify a host or network IP address and a subnet mask.

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

7. Select **Done**.

Setting firewall rule list order

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

To move a rule up or down the list:

1. Select **Menu > Options > Firewall Options** on the main screen.
2. Ensure that **Enable firewall** is selected.
3. Select **Menu > Set Rule List**. The **Firewall Rule List** screen opens.
4. Select a rule, and then select **Menu > Move**. The **Move Rule** screen opens as shown in Figure 6-4.
5. Select your preferred location.
6. Select **Done**.

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

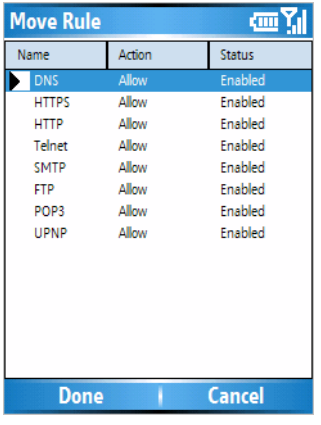


Figure 6-4. Moving a firewall rule

Deleting firewall rules

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

To delete a firewall rule:

1. Select **Menu > Options > Firewall Options** on the main screen.
2. Ensure that **Enable firewall** is selected.
3. Select **Menu > Set Rule List**. The **Firewall Rule List** screen opens.
4. Select a rule, and then select **Menu > Delete**. A confirmation prompt opens.
5. Select **Yes** on the confirmation prompt.

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

Enabling intrusion detection

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

To enable intrusion detection:

1. Select **Menu > Options > Firewall Options** on the main screen.
2. Select **Enable IDS**.
3. Select **Done**.

The IDS will block only SYN flood attacks.

Chapter 7

Filtering SMS Messages

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

This chapter covers the following topics:

SMS Anti-spam Filter Types

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

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

Mobile Security will move all blocked SMS messages to a Spam folder in your inbox. For more information, see *Handling Blocked SMS Messages* on page 7-11.

SMS Anti-spam Configuration

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

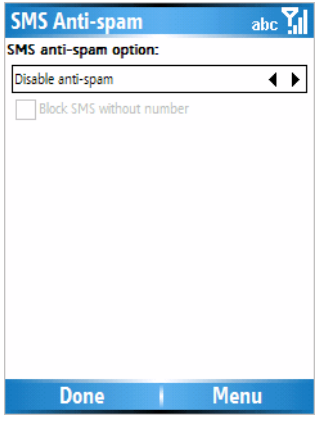


Figure 7-1. SMS Anti-spam screen

Enabling SMS anti-spam filtering

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

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

To enable an anti-spam filtering list:

1. Select **Menu > Options > SMS Anti-spam** on the main screen.
2. Under **SMS Anti-spam option**, select either **Enable approved list** or **Enable blocked list**.

Adding senders to your anti-spam list

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

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

To manually enter sender details:

1. Select **Menu > Options > SMS Anti-spam** on the main screen.
2. Ensure that an anti-spam list is enabled.
3. Select **Menu > Set Approved/Blocked List**.

   Mobile Security displays the current list entries as shown in Figure 7-2.
4. Select **Menu > Add**.

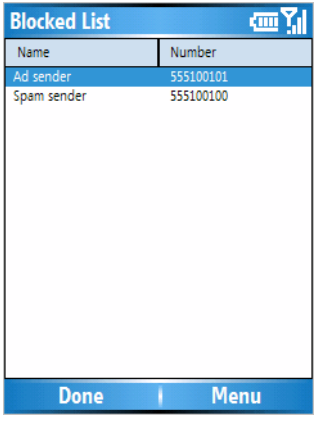


Figure 7-2. SMS anti-spam blocked list

The **Add Sender** screen opens as shown in Figure 7-3.

5. Type the name and number of the sender.
6. Select **Done** to go back to the sender list. The entry appears on the list.
7. Select **Done** to save the changes and return to the **Anti-spam Options** screen.

To import senders from your device's contact list:

1. Select **Menu > Options > SMS Anti-spam** on the main screen.
2. Ensure that an anti-spam list is enabled.
3. Select **Menu > Set Approved/Blocked List**.

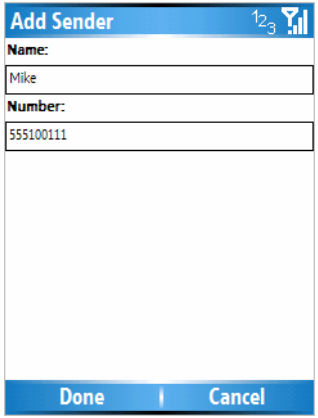


Figure 7-3. Add Sender screen

Mobile Security displays the current list entries as shown in Figure 7-4.

4. Select **Menu** > **Import**.

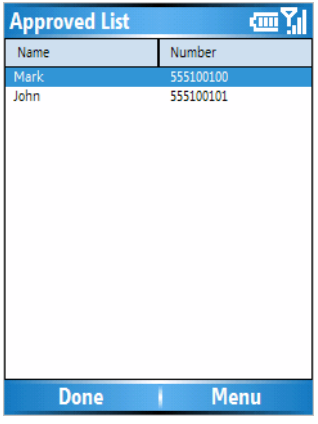


Figure 7-4. SMS anti-spam approved list

The **Import Wizard** screen opens as shown in Figure 7-5.

5. Under **When the number exists**, select one of the following options:
   - **Prompt**—inform you that a number is already on the anti-spam filtering list and allow you to specify the action
   - **Replace**—replace the entry that is currently on the anti-spam filtering list
   - **Ignore**—retain the original entry and disregard the new number
6. Select the type(s) of numbers to import under **Phone Types**.
7. Select **Next**.

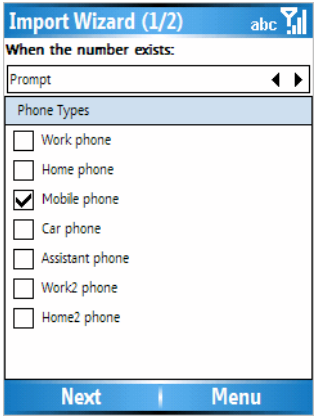


Figure 7-5. Import Wizard screen 1 of 2

Mobile Security lists all matching contacts as shown in Figure 7-6.

8. Select the contacts to import under **Select contacts** and then select **Import**.
9. Verify that your contacts have been imported.
10. Select **Done** to save the changes and return to the **Anti-spam Options** screen.

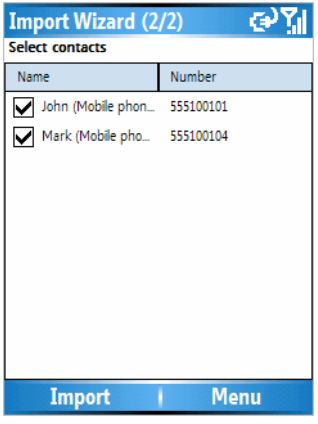


Figure 7-6. Import Wizard screen 2 of 2

Editing information on senders in your anti-spam list

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

To edit sender information:

1. Select **Menu > Options > SMS Anti-spam** on the main screen.
2. Select **Menu > Set Approved/Blocked List**. The list displays current entries.
3. Select the name of the sender.
4. Select **Menu > Edit**. The **Edit Sender** screen opens.
5. Modify the sender information and select **Done**.
6. Select **Done** again to save the changes and return to the **Anti-spam Options** screen.

Deleting senders from your anti-spam list

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

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

To delete a sender:

1. Select **Menu > Options > SMS Anti-spam** on the main screen.
2. Select **Menu > Set Approved/Blocked List**. The list displays current entries.
3. Select the name of the sender.
4. Select **Menu > Delete**.

*To delete all senders, select **Delete All**.*

5. A confirmation prompt appears. Select **Yes**.
6. Select **Done** to save the changes and return to the **Anti-spam Options** screen.

Blocking SMS messages from unidentified senders

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

To block messages from unidentified senders:

1. Select **Menu > Options > SMS Anti-spam** on the main screen.
2. Ensure that **Enable blocked list** is selected.
3. Select **Block SMS without number** as shown in Figure 7-7.
4. Select **Done**.

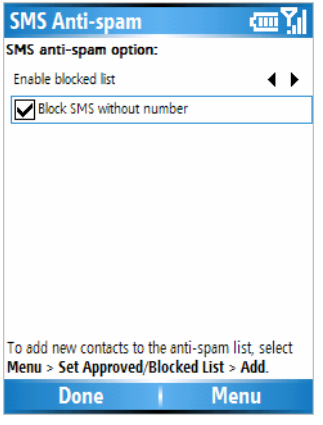


Figure 7-7. SMS Anti-spam screen

Blocking SMS messages without sender number information may filter out wanted messages. Check the Spam folder periodically to ensure that the current SMS anti-spam settings do not block messages that you want to receive. See *Handling Blocked SMS Messages on page 7-11.*

Disabling SMS anti-spam filtering

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

To disable all SMS filtering:

1. Select **Menu > Options > SMS Anti-spam** on the main screen.

2. Under **SMS Anti-spam option**, select **Disable anti-spam**.
3. Select **Done**.

Handling Blocked SMS Messages

Mobile Security moves blocked SMS messages to a Spam folder in your messaging inbox (shown in Figure 7-8). You can handle these messages as you would messages in your Inbox folder.

To access the Spam folder, select the **Folder** view while accessing your Inbox folder.

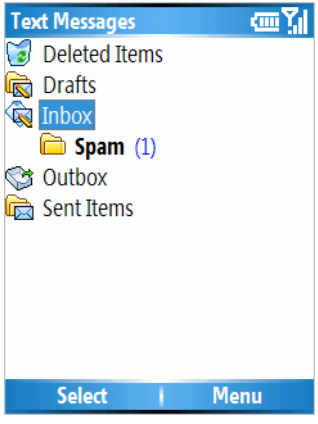


Figure 7-8. Mobile Security Spam folder

Chapter 8

Filtering WAP Push Messages

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

This chapter covers the following topics:

Understanding WAP Push Messages

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

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

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

Enabling WAP Push Protection

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

To enable WAP Push protection:

1. Select **Menu > Options > WAP Push Protection** on the main screen. The **WAP Push Protection** screen opens as shown in Figure 8-1.
2. Select **Enable protection**.
3. Select **Done**.

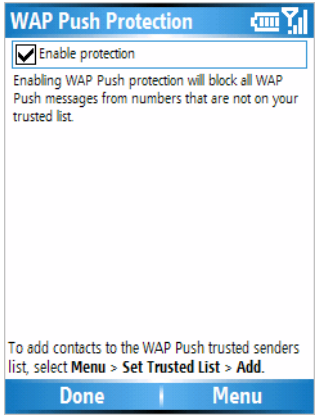


Figure 8-1. WAP Push Protection options screen

Managing the WAP Push Trusted Senders List

Mobile Security will automatically allow messages from senders on you trusted list. Whenever you receive a WAP Push message from an unknown sender, Mobile Security will prompt you to allow or block the message.

Adding trusted WAP Push senders

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

To add a sender to the trusted senders list:

1. Select **Menu > Options > WAP Push Protection** on the main screen.
2. Ensure that **Enable protection** is selected.
3. Select **Menu > Set Trusted List**.

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

4. Select **Add**. The **Add Sender** screen opens.
5. Type the name and number of the sender.
6. Select **Done**.

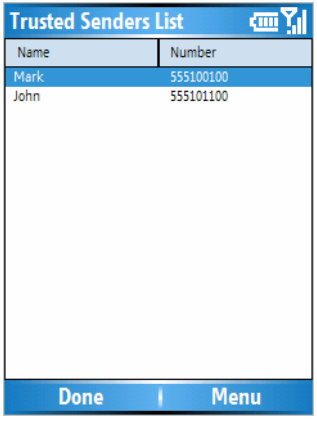


Figure 8-2. Trusted Senders List screen

*Alternatively, to add WAP Push senders to your trusted list, select **Add to trusted list** whenever Mobile Security alerts you to a WAP Push message from an unknown sender. You must accept the incoming WAP Push message to add the sender.*

Modifying information on trusted WAP Push senders

To edit trusted sender information:

1. Select **Menu > Options > WAP Push Protection** on the main screen.
2. Ensure that **Enable protection** is selected.
3. Select **Menu > Set Trusted List**. The list displays current entries.
4. Select the entry to edit.
5. Select **Menu > Edit**. The **Edit Sender** screen opens.

6. Modify the sender information and select **Done**.

Deleting trusted WAP Push senders

To delete senders from the trusted list:

1. Select **Menu > Options > WAP Push Protection** on the main screen.
2. Ensure that **Enable protection** is selected.
3. Select **Menu > Set Trusted List**. The list displays current entries.
4. Select the name of the sender.
5. Select **Menu > Delete**.

*To delete all senders, select **Delete All**.*

6. A confirmation prompt appears. Select **Yes**.
7. Select **Done** to save the changes and return to the **WAP Push Protection** screen.

Handling Blocked WAP Push Messages

Mobile Security alerts you whenever you receive WAP Push messages from senders that are not on your trusted list. Figure 8-3 shows the WAP Push alert message.

Select **No** to prevent the WAP Push messages from reaching your device. These blocked messages will not be stored on your device.

*To add an unknown WAP Push message sender to your trusted list, select **Add to trusted list** on the WAP Push alert message and select **Yes**.*

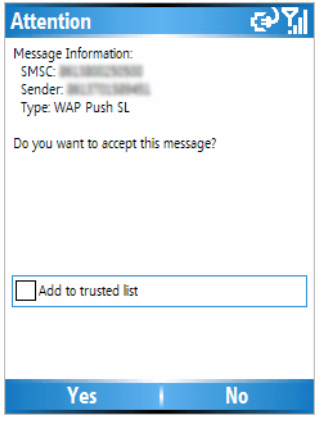


Figure 8-3. WAP Push alert message

Viewing Event Logs

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

The chapter covers the following topics:

Event Log Types

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

Scan log

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

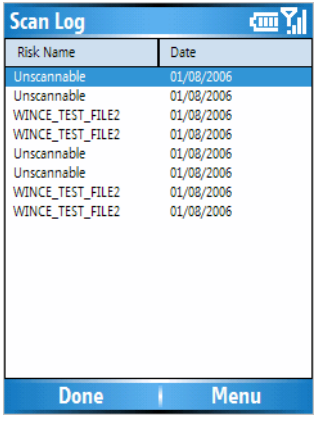


Figure 9-1. Scan log entries

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

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

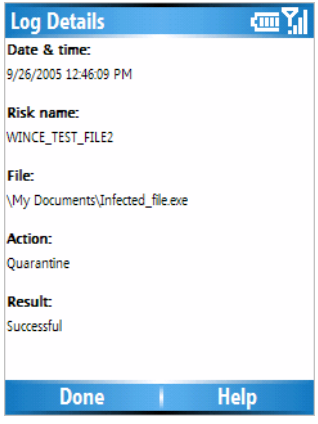


Figure 9-2. Scan log details

Task log

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

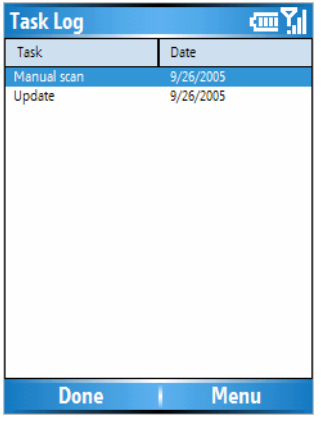


Figure 9-3. Task log entries

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

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

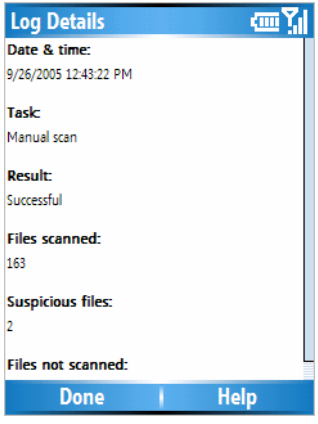


Figure 9-4. Task log details

Firewall log

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

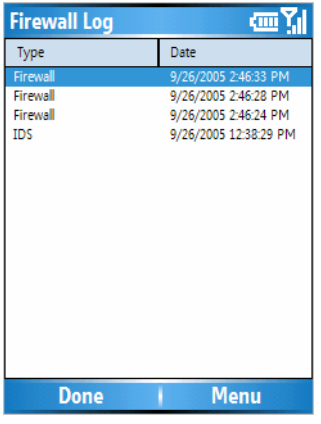


Figure 9-5. Firewall log entries

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

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

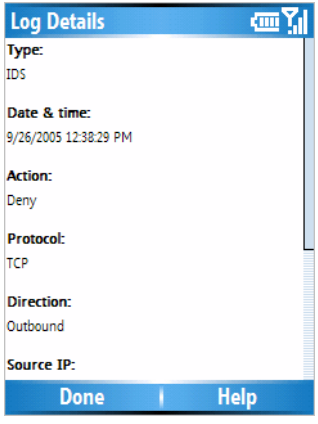


Figure 9-6. Firewall log details

Spam log

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

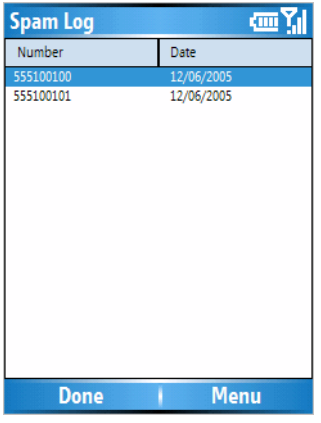


Figure 9-7. Spam log entries

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

- **Date & time**—when the SMS message was blocked
- **Description**—additional information on the event, such as the sender number

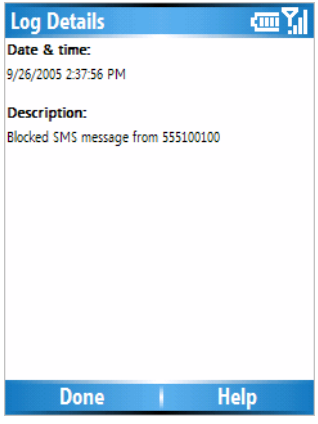


Figure 9-8. Spam log details

WAP Push log

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

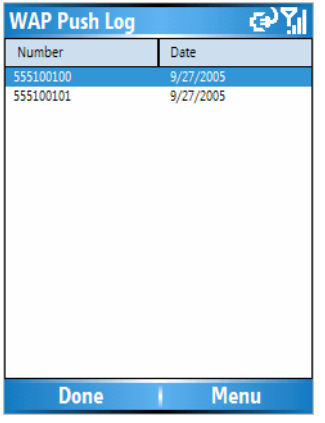


Figure 9-9. WAP Push log entries

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

- **Date & time**—when the WAP Push message was blocked
- **Description**—additional information on the event, such as the sender number

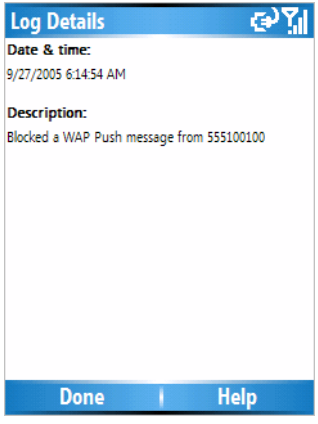


Figure 9-10. WAP Push log details

Viewing Logs

To view each log, select the log from the Event Logs submenu.

To view log entries:

1. Select **Menu > Event Logs** and then select the log type. Figure 9-11 shows the log types in the Event Logs submenu.
2. In the log screen, select the log entry you wish to view.
3. Select **Menu > View**.

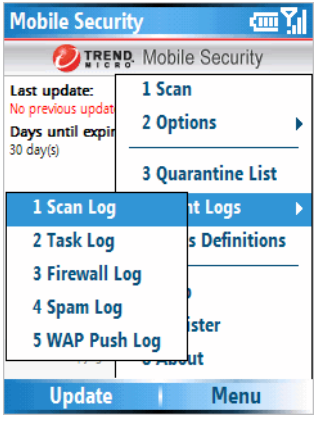


Figure 9-11. Event logs

Deleting Logs

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

To clear a log:

1. Select **Menu > Event Logs** and then select the log type.
2. Select **Menu > Clear Log**. A confirmation screen opens.
3. Select **Yes**.

Mobile Security allocates 32KB of memory space for each log type. When this limit is reached, it automatically deletes the oldest entries to accommodate new entries.

Chapter 10

Troubleshooting, FAQ, and Technical Support

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

This chapter covers the following topics:

Troubleshooting

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

Issue	Recommended Action
The device encountered a battery failure while installing Mobile Security. The installation process was stopped.	Ensure that the device has adequate power and perform the installation process again.
My battery failed while uninstalling Mobile Security. Subsequent installation efforts would always fail.	Uninstallation did not complete. Use available tools designed for your device to remove incomplete software installations.
I cannot open quarantined files.	When Mobile Security quarantines a file, it encrypts the file. You may restore the quarantined file; however, Trend Micro does not recommend this action.
Mobile Security is operating slowly.	Check the amount of storage space available on the device. If you are approaching the device's maximum memory limit, consider deleting unnecessary files and applications.
I cannot perform updates while the device is connected to a host computer.	Verify the following: • The device's proxy settings are identical to the host computer's settings • The host computer is connected to the Internet

Issue	Recommended Action
I cannot perform updates using GPRS.	Confirm that your device is connected to the Internet through a GPRS connection. If you are connected to a host computer, your device may not allow a GPRS connection. See your device's documentation for details.
I cannot import contacts from the device's contact list into my anti-spam filtering list.	Run the Import Wizard again and ensure that the import options are configured correctly. Ensure that the phone types you import match the phone types used by your contacts.
I cannot read my serial number on the Register screen.	Your device may be in flight mode. Switch to normal mode and then restart your handheld device.
I cannot receive SMS messages after installing Mobile Security.	If the approved senders list is enabled and the list is empty, all SMS messages will be blocked and moved to the Spam folder. Check the Spam folder and your anti-spam settings.
I cannot receive WAP Push messages even when I choose to accept the messages.	Your device may not support receiving WAP Push messages. Check your device's documentation to find out whether WAP Push message parsing is supported on your device.
A message pops up that requests to open a wireless connection.	This is normal if you have selected the **Wireless connection alert** option in the **Update Options** screen. You can disable this option, but you will not be warned whenever Mobile Security opens a wireless connection to check for updates.

Issue	Recommended Action
Mobile Security has been installed successfully. However, a security risk being copied could not be detected.	Check the service Activation Code (AC) you have registered; this AC may have already expired. Also, Trend Micro recommends launching Mobile Security at least once after installation. Visit the Trend Micro Web site at http://www.trendmicro.com/tmms/buy for AC registration details.
I cannot copy a file into the device.	The file may be infected and is being blocked by Mobile Security. You can disable Real-time Scan, but you will risk infecting your device.
I cannot access the Internet or other network resources.	Check your firewall settings. If the firewall protection level is set to high, all inbound and outbound traffic will be blocked. See *Using the Firewall* on page 6-1.
I cannot use the firewall or the WAP Push protection feature. I receive a message saying that the firewall or the WAP Push protection driver is not loaded.	Try restarting your device. On some devices, Mobile Security may require a restart after installation to load the firewall or the WAP Push protection driver.

Frequently Asked Questions (FAQ)

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

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

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

  Mobile Security version supports several licensing options. 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 to the same location where you installed Mobile Security.

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

  Trend Micro recommends updating program components weekly.

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

  Yes. Mobile Security can scan ZIP and Microsoft CAB files. You can configure Mobile Security to scan within up to three compression layers.

- **Can I receive or make a call while Mobile Security is performing a scan?**

  Yes. Mobile Security can scan in the background while you perform other functions on the device. You can view the logs to see details on scans and any detected viruses and security risks.

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

  No. Mobile Security can only quarantine or delete infected files.

- **Will Mobile Security log entries take up a large amount of memory space?**

  Mobile Security allows each type of log a maximum of 32KB of memory.

- **Can I open detected files on my device?**

  No. With real-time scan enabled, Mobile Security will block the opening, copying, or moving of any detected security risks. You may disable real-time scan, but you will risk infecting your device.

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

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

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

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

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

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

- **Why is my network traffic not being filtered?**

  If you are connected to a network through an ActiveSync connection, all your network traffic will not be filtered. The Mobile Security firewall cannot filter both inbound and outbound network traffic that passes through an ActiveSync connection.

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

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

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

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

Technical Support

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

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

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

Contacting Technical Support

You can contact Trend Micro by fax, 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 computer
- Network type
- Computer and device brand, model, and any additional hardware connected to your device
- Amount of memory and free space on your device
- Exact text of any error messages
- Steps to reproduce the problem

Using the Knowledge Base

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

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

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

http://esupport.trendmicro.com/

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

Sending security risks to Trend Micro

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

http://subwiz.trendmicro.com/SubWiz

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

- **Email—**the email address where you would like to receive a response from the antivirus team
- **Product—**the Trend Micro product you are currently using; if you are using multiple products, select the most relevant product or the product you use the most

- **Upload File—**Trend Micro recommends that you create a password-protected zip file (using the password `virus`) to contain the suspicious file; you can then select the password-protected zip file for upload.
- **Description—**include a brief description of the symptoms you are experiencing; our team of virus engineers will analyze the file to identify and characterize any security risks it may contain

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

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

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

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

About TrendLabs

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

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

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

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

About Trend Micro

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

Glossary

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

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

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

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

Index

Z