TREND MICRO™

TREND MICRO™ Mobile Security 8.0

Comprehensive security for enterprise handhelds

for Symbian 5th Edition

User's Guide

Endpoint Security

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

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

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

Copyright © 2004–2012 Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Release Date: July 2012

The User's Guide for Trend Micro Mobile Security for Enterprise v8.0 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

Understanding Mobile Threats 1-2
Protecting Mobile Devices 1-2
Mobile Security Overview 1-3
Mobile Security Features 1-3
Upgrading to Mobile Security 8.0 1-4

Chapter 2: Installing Trend Micro Mobile Security

Before Installing 2-2
Manual Installation Methods 2-2
System Requirements 2-4
Host Computer Requirements 2-4
Installing Mobile Security 2-5
Manual Registration 2-8
Uninstallation 2-10

Chapter 3: Getting Started with Trend Micro Mobile Security

Understanding the Mobile Security Interface 3-3
Main Screen 3-4
Product License 3-4
Menu Items 3-6
Reviewing Default Protection Policies 3-7
Updating Anti-Malware Components 3-11
Scanning for Malware 3-11

Chapter 4: Updating Anti-Malware Components

Connecting to the Mobile Security Management Server 4-2
Updating Program Components 4-3
Scheduled Updates 4-4
Manual Updates 4-5

Chapter 5: Scanning for Malware

Anti-Malware Scan Types 5-3
Manual Scan 5-3
Real-Time Scan 5-4

Enabling Real-Time Scan 5-4
Setting the Action for Infected/Suspicious Files 5-5

Card Scan 5-5

Scan Results 5-6
Viewing Scan Results 5-6
Handling Infected/Suspicious or Unscannable Files 5-7

Quarantined Files 5-9

Advanced Anti-Malware Policies 5-10
Scanning Compressed Files 5-10
Configuring Scan Policies for Compressed Files 5-11

Information About Mobile Malware 5-12

Chapter 6: Using the Firewall

Understanding Firewalls 6-2

Understanding Mobile Security Firewall Filtering 6-2
Predefined Protection Levels 6-3
Firewall Rules 6-4

Enabling the Firewall 6-7

Configuring the Firewall Protection Level 6-8

Advanced Firewall Policies 6-9
Creating Firewall Rules 6-9
Setting Firewall Rule List Order 6-13
Deleting Firewall Rules 6-14
Enabling Intrusion Detection 6-16

Chapter 7: Filtering SMS Messages

SMS Anti-Spam Filter Types 7-2

SMS Anti-Spam Configuration 7-3
Enabling SMS Anti-Spam Filtering 7-3
Adding Senders to the Anti-Spam List. 7-5
Editing Sender Information in the Anti-Spam List 7-8
Deleting Senders from the Anti-Spam List 7-8
Blocking SMS Messages from Unidentified Senders 7-9
Disabling SMS Anti-Spam Filtering 7-10

Handling Blocked SMS Messages 7-11

Chapter 8: Filtering WAP Push Messages

Understanding WAP Push Messages 8-2

Enabling WAP Push Protection 8-3

Enabling WAP Push Notification 8-3

Managing the WAP Push Trusted Senders List 8-4
Adding Trusted WAP Push Senders 8-4
Modifying Information on Trusted WAP Push Senders 8-5
Deleting Trusted WAP Push Senders 8-6
Handling Blocked WAP Push Messages 8-7

Chapter 9: Viewing Event Logs

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

Chapter 10: Troubleshooting, FAQ, and Technical Support

Troubleshooting 10-2
Frequently Asked Questions (FAQ) 10-6
Technical Support 10-8

Contacting Technical Support 10-8
Using the Knowledge Base 10-9
Sending Security Risks to Trend Micro 10-11
About TrendLabs 10-12
About Trend Micro 10-13

Glossary

Index

Chapter 1

Introducing Trend Micro Mobile Security

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

This chapter covers the following topics:

- *Understanding Mobile Threats* on page 1-2
- *Protecting Mobile Devices* on page 1-2
- *Mobile Security Overview* on page 1-3
- *Mobile Security Features* on page 1-3

Understanding Mobile Threats

With the standardization of platforms and their increasing connectivity, mobile 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, mobile devices are now susceptible to hacking and denial of service (DoS) attacks. Mobile 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 Mobile Devices

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

- Use an anti-malware product on the mobile device and computers you use to connect to the device.
- If you connect your mobile 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 Overview

Trend Micro™ Mobile Security is a comprehensive security solution for your mobile device. Mobile Security incorporates the Trend Micro anti-malware technologies to effectively defend against the latest mobile threats. Additionally, the integrated firewall and filtering functions enable Mobile Security to effectively block unwanted network communication (such as SMS messages and WAP push mails) to mobile devices.

Mobile Security Features

Mobile Security offers the following features:

- Scheduled or manual component updates from the Trend Micro Mobile Security Management server to ensure up-to-date scan engine, pattern, and program versions.
- Automatic configuration synchronization with the Mobile Security Management server to meet company network security policies.
- Award-winning anti-malware scanning technology to scan for mobile malware and other malware.

- Automatic and regular component updates.
- Robust firewall and intrusion detection system (IDS) features to block unwanted network communication to your mobile devices and prevent denial of service (DoS) attacks.
- SMS Anti-Spam prevents anonymous spam from reaching your inbox.
- WAP Push Protection prevents mobile devices from receiving unwanted content.
- Event logs on scanning results, detected malware, and matched firewall rules and the actions performed.

Upgrading to Mobile Security 8.0

You can upgrade Mobile Security version 7.1 to 8.0 on mobile devices without uninstalling the previous version. The Setup program automatically removes Mobile Security 7.1 before installing Mobile Security 8.0.

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:

- *Before Installing* on page 2-2
- *System Requirements* on page 2-4
- *Installing Mobile Security* on page 2-5
- *Manual Registration* on page 2-8
- *Uninstallation* on page 2-10

Before Installing

You can skip the installation section if your network administrator has already installed and configured the Mobile Device Agent on your mobile device.

Before you begin, obtain the following information from your network administrator:

- installation method
- registration information (if manual registration is required)

Mobile Device Agent does not support the backup/restore function on Symbian platforms.

Manual Installation Methods

If you are asked to install Mobile Security manually, your network administrator will tell you the installation method to use and provide you with the requirement information. You can manually install Mobile Security on your mobile device using one of the following methods:

- Clicking the URL in an SMS message
- Using a memory card
- Executing the setup file (this method may require manual registration to the Mobile Security Management server)

Depending on your installation method, make sure you have the required information provided by your network administrator.

TABLE 2-1. Required information for manual installation

METHOD	REQUIRED INFORMATION
Installation SMS Message	Installation SMS message in the inbox on your mobile device
Memory Card	A memory card with the Mobile Device Agent setup file in the root folder
Executing Setup File	Mobile Device Agent setup file A memory card or a host computer with PC Suite Registration information (such as the server IP address and service port number)

You can only use the memory card installation method once. For example, if you have installed Mobile Device Agent on your mobile device using a memory card before, you cannot install Mobile Device Agent again on your mobile device using a memory card.

System Requirements

Before installing and using Mobile Security, ensure that your mobile device and the host computer to which you are connecting meets the following requirements:

TABLE 2-2. Mobile device requirements

Operating system	Symbian OS 9.x S60 5th Edition
Storage space	Minimum 1.88MB free space on your mobile device
Memory	1.77MB minimum free memory; 3MB recommended

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

Host Computer Requirements

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

Installing Mobile Security

This section shows you how to install Mobile Device Agent on your mobile device.

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

Your network administrator may provide you a memory card with the Mobile Security setup file. Or, the network administrator may store the setup file onto your memory card.

To install Mobile Security using a memory card

1. Insert the memory card into your mobile device. Setup automatically installs Mobile Security on your mobile device.
2. After the installation is complete, restart your mobile device when prompted. Mobile Security is added to the **Application** menu.
3. Verify that the **Server IP/Hostname** and **Server Port** fields on the **Register** screen display the valid information.
4. Tap **Register** to register your mobile device to the Mobile Security Management server.

Memory card installation method is not available if you want to re-install or upgrade Mobile Security 7.0 on your mobile device. In this case, you should use the manual installation method.

To install Mobile Security using the notification SMS message:

1. Make sure your mobile device can connect to the Mobile Security Management server.
2. Check the inbox on the mobile device. Your mobile device should have received three SMS messages from the Mobile Security Management server. Open the SMS message with a URL.

Do not delete the registration SMS message from the inbox. Mobile Device Agent uses information in the SMS message to register to the Mobile Security Management server. If you have accidentally deleted this SMS message, contact your network administrator for assistance.

3. Access the URL to download the Mobile Device Agent setup file.

After the download is complete, setup automatically installs Mobile Device Agent on your mobile device. After the installation is complete, your mobile device automatically restarts. Mobile Security is added to the **Application** menu.

After the installation process is completed, the **Server IP/Hostname** and **Server Port** fields on the **Register** screen display the valid information. Tap **Register** to register your mobile device to the Mobile Security Management server. After the registration is completed successfully, the mobile device automatically deletes the registration SMS message.

To manually install Mobile Security by executing the setup file on a host computer:

1. Copy the setup file `MobileSecurity_S60.sis` to the host computer.
2. Connect your mobile device to the host computer with PC Suite.
3. On the host computer, open the installation file. The PC Suite installer opens and prompts you to begin the installation.
4. Start the installation. A message appears to inform you to check your mobile device for further instructions.
5. Click **OK** on the prompt.
6. Follow the instructions on your mobile device to complete the installation.
7. Mobile Security will prompt you to restart your mobile device. Restart your mobile device to ensure that all product modules are loaded. Mobile Security is added to the **Application** menu.
8. Register your mobile device to the Mobile Security Management server (refer to *Manual Registration* on page 2-8 for more information).

To manually install Mobile Security by executing the setup file on the mobile device:

1. Copy the setup file `MobileSecurity_S60.sis` to your mobile device. You can use PCsuite, Bluetooth, or a memory card to transfer the file.
2. On your mobile device, navigate to the location of the setup file.
3. Open the setup file to start installing Mobile Device Agent.
4. After the installation is complete, you will receive a prompt to restart your device. Mobile Security is added to the **Application** menu.

5. Register your mobile device to the Mobile Security Management server (refer to *Manual Registration* on page 2-8 for more information).

Manual Registration

Register your mobile device to the Mobile Security Management server to obtain the licenses for Mobile Security on your mobile device.

If your mobile device is not registered to the Mobile Security Management server, the **Register** screen displays the first time you launch Mobile Security. You should have the registration information (such as the Host and port number of the Mobile Security Management server) provided by your network administrator.

If you do not wish to register your mobile device to the Mobile Security Management server at this time, you can still use Mobile Security on your mobile device with a trial license. Trial expiration varies according to the product version. The trial license allows you to use certain basic features like: SMS Anti-Spam, WAP push protection, malware scanning and firewall features. Component updates are not allowed in the trial version.

To manually register Mobile Device Agent to the Mobile Security Management server:

1. On the main screen select **Options** > **Register**. The registration screen opens.
2. Configure the fields in the screen.
   - **Device Name**—type a descriptive name for your mobile device. This name identifies your mobile device on the Mobile Security Management server.

- **Host**—type the Host of the Mobile Security Management server. This information is provided by your network administrator.
- **Port**—type the Web server port number on the Mobile Security Management server. For example, 80. This information is provided by your network administrator.
- **Domain Username** and **Domain Password**—type your network domain name and password.

3. Select **Option > Register**. If prompted, select an access point to continue. The registration process may take several minutes depending on your network connection.
4. After the registration is completed successfully, the main Mobile Device Agent screen displays.

For more information on product licenses, refer to *Product License* on page 3-4.

Uninstallation

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

To uninstall directly on the mobile device:

1. On the mobile device, go to **Menu** > **Tools** > **Application manager**.
2. Scroll to **Mobile Security**.
3. Select **Options > Remove**.
4. When prompted for confirmation, select **Yes**.
5. When Mobile Security prompts you to save policies, select either of the following:
   - **Yes** to save your current policies, including firewall rules and anti-spam lists, so you can use them when you reinstall Mobile Security.
   - **No** to delete your current policies.

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, and the default product policies.

This chapter covers the following topics:

- *Understanding the Mobile Security Interface* on page 3-3
- *Product License* on page 3-4
- *Reviewing Default Protection Policies* on page 3-7

- *Updating Anti-Malware Components* on page 3-11
- *Scanning for Malware* on page 3-11

Understanding the Mobile Security Interface

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

- Main Screen on page 3-4
- Menu Items on page 3-6

Main Screen

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

TABLE 3-1. Main screen interface items

INTERFACE ITEM	ACTION
1	Enable or disable the real-time scan
2	Select between predefined firewall protection levels or disable the firewall
3	Access product features and policies

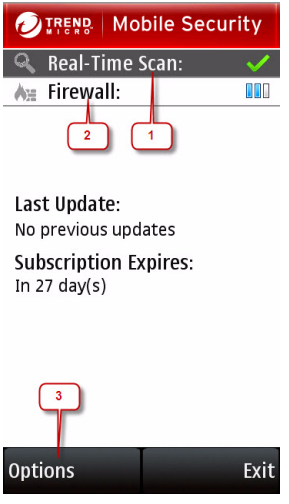

Figure 3-1. Main screen

Product License

Depending on the type of license for Mobile Security, features available vary after license expiration.

If the trial license for Mobile Security expires, all features are disabled on your mobile device. If the full license for Mobile Security expires, you can still use certain basic features like: SMS Anti-Spam, WAP push protection, malware scanning and firewall features.

Component updates are not allowed after the license expires. However, malware scans may use out-of-date anti-malware components and therefore may not detect the latest security risks.

Menu Items

The Main Screen **Options** menu enables you to access the product features. The menu items are shown in *Figure 3-2* and the actions they perform are described in *Table 3-2*.

TABLE 3-2. Menu items on the main screen

MENU ITEM	ACTION
Scan Now	Scan your mobile device for malware
Update	Check for updates
Settings	Configure product settings
Logs	View event logs
Quarantine List	Access quarantined files
Malware Definitions	View definitions of known mobile malware

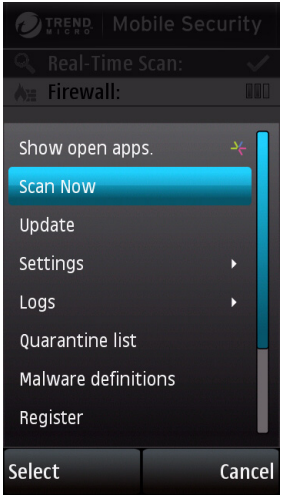

Figure 3-2. Main screen options

TABLE 3-2. Menu items on the main screen (Continued)

MENU ITEM	ACTION
Register	Register the product
About	View the About screen
Help	View the Help

Reviewing Default Protection Policies

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

Your network administrator may not allow you to change Mobile Device Agent policies on your mobile device.
The Mobile Security Management server may control the SMS anti-spam and WAP Push protection features on your mobile device.

TABLE 3-3. Default protection settings

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

TABLE 3-3. Default protection settings (Continued)

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

TABLE 3-3. Default protection settings (Continued)

FEATURE	DEFAULT SETTING	RESULTING ACTION
SMS Anti-Spam	Disabled	Product allows all SMS messages to reach the messaging inbox, except for messages from specified senders.
WAP Push Protection	Disabled	Product does not filter WAP Push messages and allows all messages to reach the mobile device. You can enable or disable this feature on your mobile device.

Updating Anti-Malware Components

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

To update Mobile Security:

1. Select **Options > Update**. Mobile Security prompts you to specify a connection access point.
2. Select a valid access point. Mobile Security connects to the Mobile Security Management server through the selected access point.

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

Scanning for Malware

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

For more information on Mobile Security anti-malware capabilities, see *Scanning for Malware* on page 5-1.

Chapter 4

Updating Anti-Malware Components

To stay protected against the latest mobile malware and other malware, update the anti-malware components regularly.

This chapter covers the following topics:

- *Connecting to the Mobile Security Management Server* on page 4-2
- *Updating Program Components* on page 4-3

Connecting to the Mobile Security Management Server

To update Mobile Security, you must connect to the Mobile Security Management server on the intranet or through the Internet. You can configure the connection settings by specifying an access point.

To configure connection settings:

1. Tap **Options > Settings > Advanced settings**. The **Advanced** screen opens.
2. Tap the **Access point** field to select an access point.

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

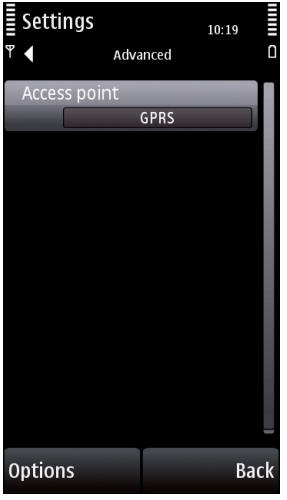

Figure 4-1. Connection settings screen

Updating Program Components

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

TABLE 4-1. Update types

TYPE		DESCRIPTION
Manual		User-initiated; you can run these updates anytime.
Scheduled	Automatic	This update runs whenever you start a network connection on your mobile device if the specified update interval since the last successful update check has elapsed.
	Forced	This update runs when the specified interval has elapsed since the last successful download and installation of new components. Forced updates will open the default wireless connection if your mobile device is not connected to the Mobile Security Management server.

Scheduled Updates

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

To configure the intervals between scheduled updates:

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

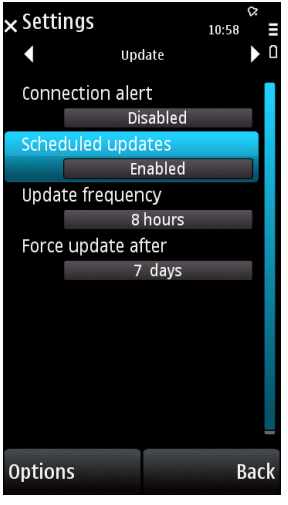

Figure 4-2. Update settings screen

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

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

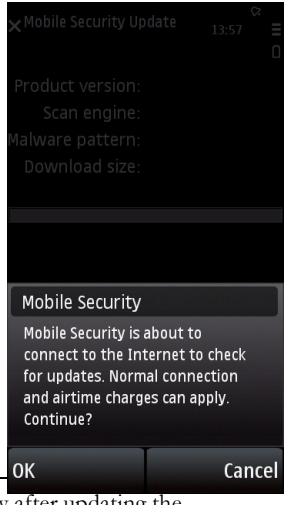

Figure 4-3. Wireless connection alert

Manual Updates

To perform a manual update:

- Tap **Options > Update**. Mobile Security prompts you for the access point or automatically connects to the Internet through the predefined access point.

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 5-3.

Chapter 5

Scanning for Malware

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

This chapter covers the following topics:

- *Anti-Malware Scan Types* on page 5-3
- *Manual Scan* on page 5-3
- *Real-Time Scan* on page 5-4
- *Card Scan* on page 5-5

- *Scan Results* on page 5-6
- *Quarantined Files* on page 5-9
- *Advanced Anti-Malware Policies* on page 5-10
- *Information About Mobile Malware* on page 5-12

Anti-Malware Scan Types

Mobile Security offers the following anti-malware scan types:

TABLE 5-1. Anti-Malware 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

Manual Scan

A manual scan will scan all files on your mobile device for malware. To run a manual scan, select **Options > Scan** on the main screen.

The scan results screen displays a list of any infected and unscannable files. You can choose to delete or quarantine these files. For more information, see *Handling Infected/Suspicious or Unscannable Files* on page 5-7.

Real-Time Scan

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

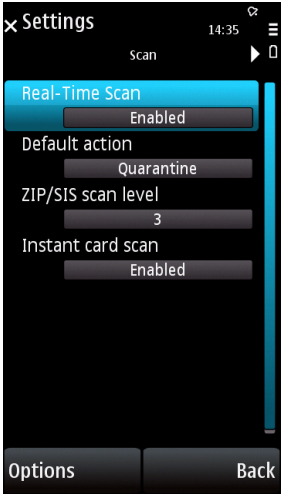

Figure 5-1. Scan settings screen

Enabling Real-Time Scan

Enabling real-time scan enhances malware protection on your mobile device.

To enable real-time scan:

1. Tap **Options > Settings > Scan** on the main screen. The **Scan** screen opens.
2. Tap **Real-time scan** to select **Enabled**.

To disable the real-time scanner, select **Disabled** under **Real-time scan** in the **Scan settings** screen. If you disable the real-time scanner, proactive protection is unavailable on your mobile device.

Setting the Action for Infected/Suspicious Files

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

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

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

Card Scan

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

To enable card scan:

1. Tap **Options > Settings > Scan** on the main screen. The **Scan** screen opens.
2. Tap **Instant card scan** to select **Enabled**.

Scan Results

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

Viewing Scan Results

After a manual or card scan, Mobile Security displays a list of infected/suspicious and unscannable files. You can either quarantine or delete these files as discussed in *Handling Infected/Suspicious or Unscannable Files* on page 5-7.

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

Figure 5-2. Scan results

TABLE 5-2. Scan result items

SCAN RESULT ITEM	DESCRIPTION
Suspicious files	Files found to contain mobile malware
Unscannable files	Files compressed within an archive that cannot be accessed; these files may be compressed within too many layers of compression, password-protected, or too large to be extracted on the mobile device

To view details on an infected/suspicious or unscannable file, tap the the file.

For more information on setting the number of compression layers to scan, see *Advanced Anti-Malware Policies* on page 5-10.

Handling Infected/Suspicious or Unscannable Files

If you exit the scan results screen without quarantining or deleting suspicious files, these files stay in your mobile device and may cause damage to other files or the actual mobile device itself.

To delete or quarantine an infected/suspicious or unscannable file:

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

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

Quarantined Files

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

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

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

To restore files from quarantine:

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

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

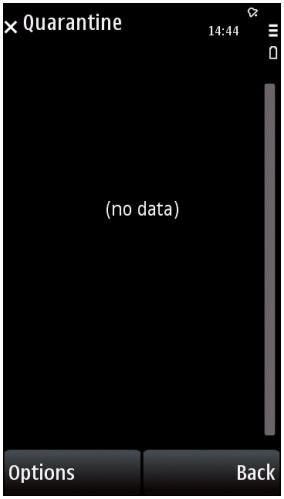

Figure 5-3. Quarantine list

Advanced Anti-Malware Policies

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

Scanning Compressed Files

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

You can set Mobile Security to extract files with 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 anti-malware scanners. Although such files may not be scanned if you select a low maximum number of compression layers, they will be tagged unscannable and you will be able to delete or quarantine them.

Configuring Scan Policies for Compressed Files

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

To configure the compression layers to scan:

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

The item **Default action** applies only to the real-time scan. See *Setting the Action for Infected/Suspicious Files* on page 5-5.

Information About Mobile Malware

To view information about known mobile malware, tap **Options > Malware definitions** on the main screen. The **Malware definitions** screen opens as shown in *Figure 5-4*.

To view additional details on malware, scroll to the name of the malware and press the select key.

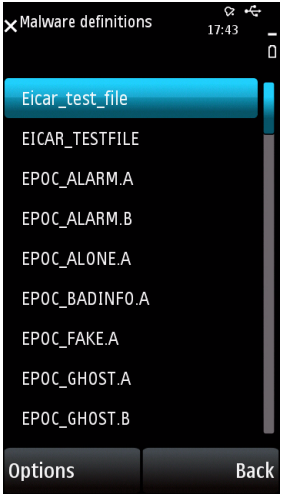

Figure 5-4. Malware definitions screen

Chapter 6

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 mobile device.

This chapter covers the following topics:

- *Understanding Firewalls* on page 6-2
- *Understanding Mobile Security Firewall Filtering* on page 6-2
- *Enabling the Firewall* on page 6-7
- *Configuring the Firewall Protection Level* on page 6-8
- *Advanced Firewall Policies* on page 6-9

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 mobile device. You can control the ports that applications running on your mobile 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 mobile device and the addresses to which your mobile device can connect.

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

Ports are typically associated with certain applications and services. See *Firewall Rules* on page 6-4 for more information.

Understanding Mobile Security Firewall Filtering

Mobile Security provides two filtering methods with the firewall:

- Predefined protection levels
- Firewall rules

Predefined Protection Levels

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

TABLE 6-1. Predefined protection levels

PROTECTION LEVEL	MODE	DESCRIPTION
Low	Open	All inbound and outbound traffic is allowed.
Normal	Stealth	All outbound traffic is allowed; all inbound traffic is blocked.
High	Locked	All inbound and outbound traffic is blocked.

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

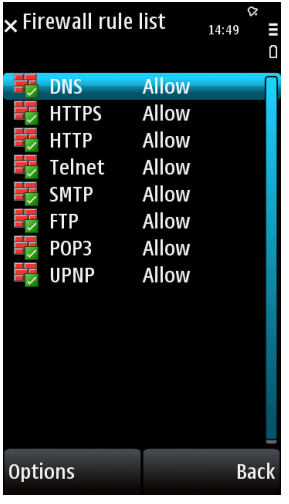

Figure 6-1. Firewall rule list

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

TABLE 6-2. Default firewall rules

RULE	PORT	COMMON USAGE	DEFAULT FIREWALL POLICY
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

You can modify the default firewall rules and create your own rules. For more information, see *Advanced Firewall Policies* on page 6-9.

Enabling the Firewall

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

To enable the firewall:

1. Tap **Options > Settings > Firewall** on the main screen. The **Firewall** screen opens.
2. Tap **Firewall** to select **Enabled**.

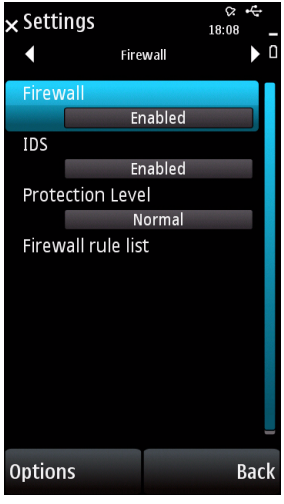

Figure 6-2. Firewall settings screen

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 6-3.

To configure your firewall protection level:

1. Tap **Options > Settings > Firewall** on the main screen.
2. Ensure that **Firewall** is enabled.
3. Tap **Protection level** to select your preferred protection level.
4. Tap **OK**.

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

Advanced Firewall Policies

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

To create a firewall rule:

1. Tap **Options > Settings > Firewall** on the main screen.
2. Ensure that **Firewall** is enabled.
3. Tap **Firewall rule list**.
4. Tap **Options > New rule**. The **Rule details** screen opens as shown in *Figure 6-3*.

If a new rule shares many similar characteristics with an existing rule, you can select the existing rule, select **Menu > Duplicate**, and then modify the duplicated rule as appropriate.

5. Provide a unique name for the rule.
6. Provide the corresponding details on the **Rule details** screen. For information on the items on the screen, see *Table 6-3*.

Figure 6-3. Rule details screen

TABLE 6-3. Rule details screen items

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 (Continued)

ITEM	OPTIONS	DEFINITION
Port(s)	• All ports • Port range • Specific port(s)	Determines the ports in the mobile 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 **ICMP** or **All** is selected under **Protocol**, you cannot specify ports.
IP address(es)	• All IP addresses • Single IP • IP 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 network IP address and a subnet mask.

7. Select **Back**.

Setting Firewall Rule List Order

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

To move a rule up or down the list:

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

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

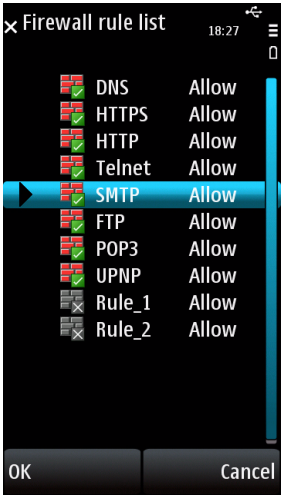

Figure 6-4. Firewall rule list with move pointer

Deleting Firewall Rules

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

To delete a firewall rule:

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

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

Enabling Intrusion Detection

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

To enable intrusion detection:

1. Tap **Options > Settings > Firewall** on the main screen.
2. Ensure that **Firewall** is enabled.
3. Tap **IDS** to select **Enabled**.

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

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* on page 7-2
- *SMS Anti-Spam Configuration* on page 7-3
- *Handling Blocked SMS Messages* on page 7-11

SMS Anti-Spam Filter Types

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

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

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

SMS Anti-Spam Configuration

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

If you are unable to control the configuration on your mobile device, it indicates that the configuration must be controlled by the server. Contact your administrator for assistance.

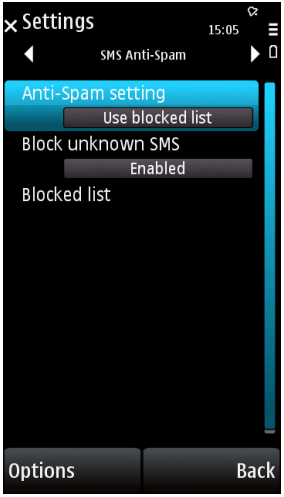

Figure 7-1. SMS Anti-Spam settings screen

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

To enable an anti-spam filtering list:

1. Tap **Options > Settings > SMS Anti-Spam** on the main screen.
2. Tap **Anti-Spam setting** to select either **Use approved list** or **Use blocked list**. Mobile Security displays the selected filtering list as soon as you enable it.

Adding Senders to the 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. Tap **Options > Settings > SMS Anti-Spam** on the main screen.
2. Ensure that an anti-spam list is enabled.
3. Tap **Approved/Blocked list**. Mobile Security displays the current list entries as shown in *Figure 7-2*.
4. Tap **Options > New entry**.

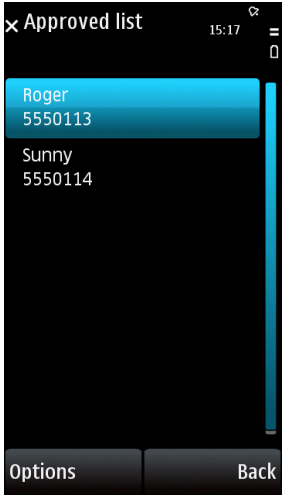

Figure 7-2. SMS Anti-Spam approved list

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

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

To import senders from your device's contact list:

1. Tap **Options > Settings > SMS Anti-Spam** on the main screen.
2. Ensure that an anti-spam list is enabled.
3. Tap **Approved/Blocked list**. Mobile Security displays the current list entries.
4. Tap **Options > Import**.

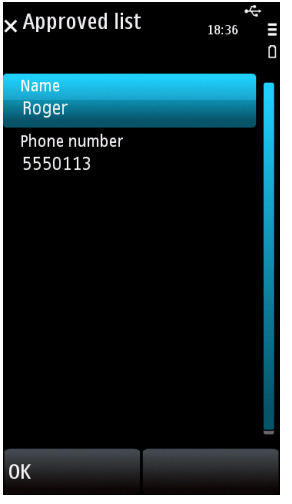

Figure 7-3. SMS Anti-Spam approved list entry

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

5. Select the contacts to import by:
   - Tapping a contact
   - Choosing all contacts by tapping **Options > Select all**
6. Tap **Options > Import**.
7. Verify that your contacts have been imported.

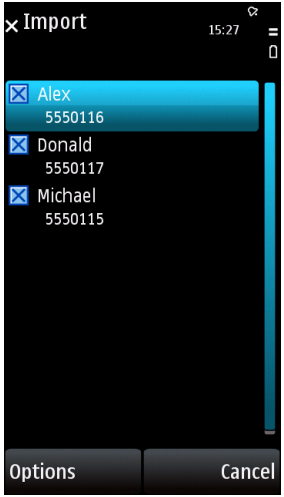

Figure 7-4. Import screen

Editing Sender Information in the Anti-Spam List

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

To edit sender information:

1. Tap **Options > Settings > SMS Anti-Spam** on the main screen.
2. Ensure that an anti-spam list is enabled.
3. Tap **Approved/Blocked list**. Mobile Security displays the current list entries.
4. Tap the name of the sender.
5. Tap **Options > Edit**.
6. Modify the sender information and tap **OK**.

Deleting Senders from the 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. Tap **Options > Settings > SMS Anti-Spam** on the main screen.
2. Ensure that an anti-spam list is enabled.
3. Tap **Approved/Blocked list**. Mobile Security displays the current list entries.
4. Tap the name of the sender.
5. Tap **Options > Delete**.

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

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

Blocking SMS Messages from Unidentified Senders

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

To block messages from unidentified senders:

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

3. Tap **Block unknown SMS** to select **Enabled** as shown in *Figure 7-5*.

Blocking SMS messages that do not have sender number information may filter out messages that you want to receive. Check the Spam folder periodically to ensure that the current SMS anti-spam settings do not block messages that you want to receive. See *Handling Blocked SMS Messages* on page 7-11.

Figure 7-5. SMS Anti-Spam with Block unknown SMS enabled

Disabling SMS Anti-Spam Filtering

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

To disable all SMS filtering:

1. Tap **Options > Settings > SMS Anti-Spam** on the main screen.
2. Tap **Anti-Spam setting**.
3. Tap **Disable anti-spam**.
4. Tap **OK**.

Handling Blocked SMS Messages

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

To access messages in the Spam folder:

1. Go to **Menu > Messaging**.
2. Tap **My folders**.
3. Tap **Spam**.

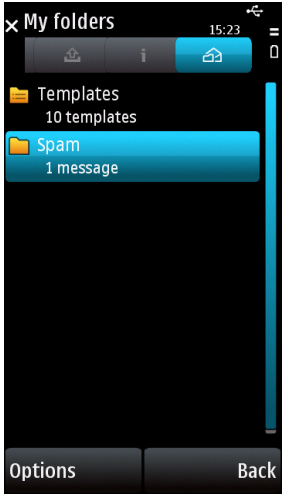

Figure 7-6. Spam folder

Chapter 8

Filtering WAP Push Messages

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

This chapter covers the following topics:

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

Understanding WAP Push Messages

WAP Push is a powerful method of delivering content to mobile devices automatically. It may be used to deliver mobile-related content such as ringtones, news, email, and mobile device policies. Because of this ability to deliver content to mobile devices, WAP Push can deliver unsolicited or unwanted content, including malware 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 mobile 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 mobile 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. Tap **Options > Settings > WAP Push Protection** on the main screen. The **WAP Push** screen opens as shown in *Figure 8-1*.
2. Tap **WAP Push Protection** to select **Enabled**.

If you are unable to control the configuration on your mobile device, it indicates that the configuration must be controlled by the server. Contact your administrator for assistance.

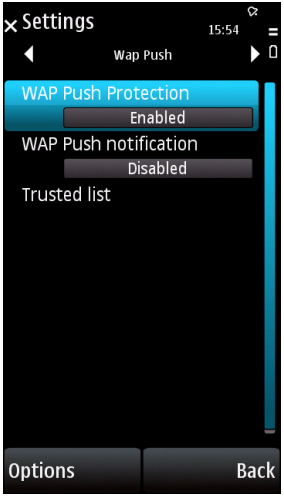

Figure 8-1. WAP Push Protection settings screen

Enabling WAP Push Notification

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

To enable WAP Push notification:

1. Tap **Options > Settings > WAP Push Protection** on the main screen. The **WAP Push Protection** settings screen opens.
2. Ensure that **WAP Push Protection** is enabled.
3. Tap **WAP Push notification** to select **Enabled**.

Managing the WAP Push Trusted Senders List

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

Adding Trusted WAP Push Senders

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

To add a sender to the trusted senders list:

1. Tap **Options > Settings > WAP Push Protection** on the main screen. The **WAP Push Protection** settings screen opens.
2. Ensure that **WAP Push Protection** is enabled.
3. Tap **Trusted list**.

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

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

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

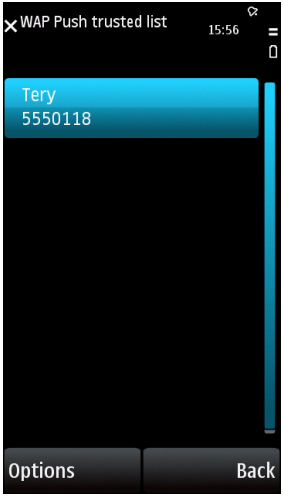

Figure 8-2. WAP Push trusted list

Modifying Information on Trusted WAP Push Senders

To edit trusted sender information:

1. Tap **Options > Settings > WAP Push Protection** on the main screen. The **WAP Push** screen opens.
2. Ensure that **WAP Push Protection** is enabled.
3. Tap **Trusted list**.
4. Tap the entry to edit.
5. Tap **Options > Edit**.

6. Modify the sender information and tap **OK**.

Deleting Trusted WAP Push Senders

To delete senders from the trusted list:

1. Tap **Options > Settings > WAP Push Protection** on the main screen. The **WAP Push** screen opens.
2. Ensure that **WAP Push Protection** is enabled.
3. Tap **Trusted list**.
4. Tap the entry to delete.
5. Tap **Options > Delete**.

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

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

Handling Blocked WAP Push Messages

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

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

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

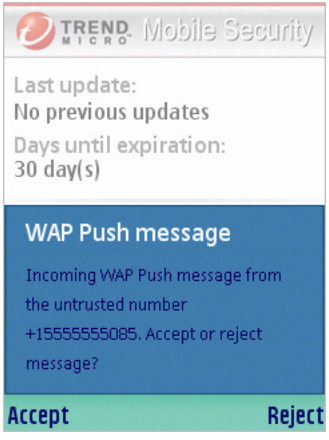

Figure 8-3. WAP Push alert message

For information on enabling WAP Push notification, see *Enabling WAP Push Notification* on page 8-3.

Chapter 9

Viewing Event Logs

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

The chapter covers the following topics:

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

Event Log Types

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

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

Scan Log

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

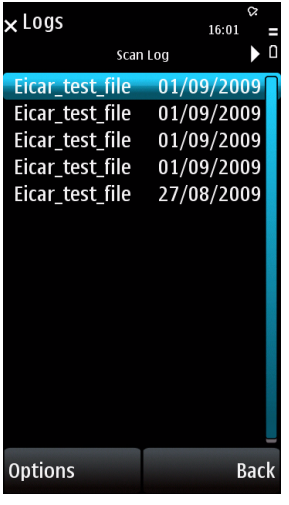

Figure 9-1. Scan log entries

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

- **Found**—when the malware was detected
- **Risk name**—the name of the malware
- **File**—the name of the infected/suspicious file
- **Action**—whether the file was quarantined, deleted, or no action taken
- **Result**—whether the action was successfully completed

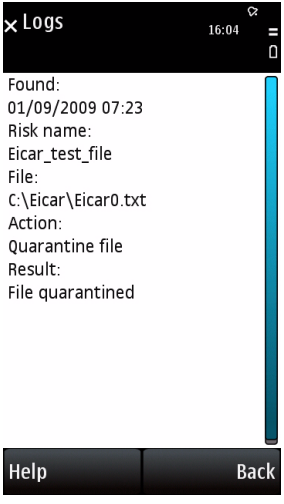

Figure 9-2. Scan log entry details

Task Log

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

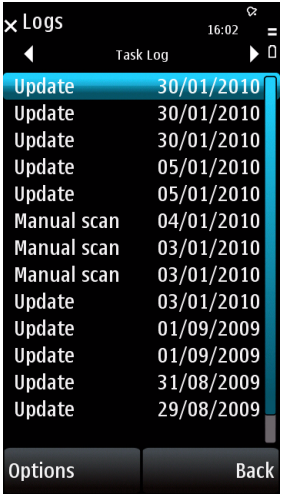

Figure 9-3. Task log entries

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

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

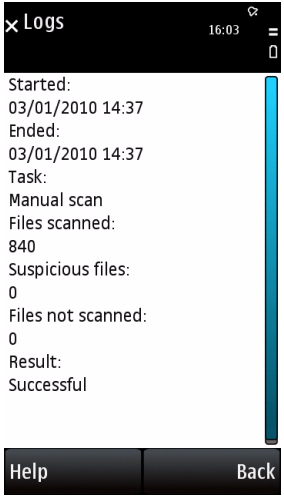

Figure 9-4. Task log entry details

Firewall Log

Mobile Security generates an entry in the firewall log (shown in *Figure 9-5*) when one of the following occurs:

- a connection attempt matches a firewall rule with the rule action of "Log Only"
- the predefined protection level blocks a connection attempt
- the IDS blocks a connection attempt

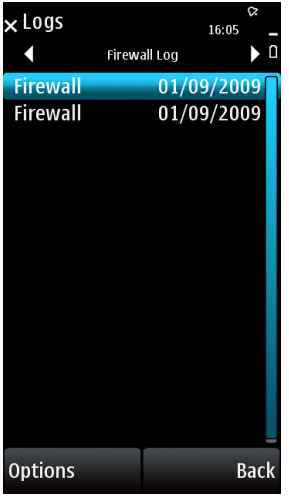

Figure 9-5. Firewall log entries

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

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

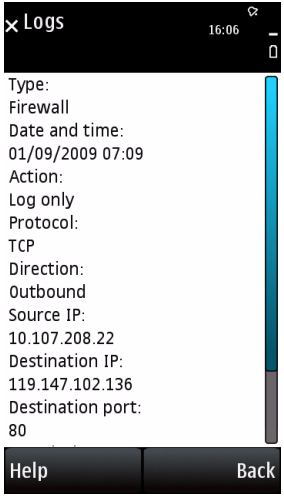

Figure 9-6. Firewall log entry details

Spam Log

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

Figure 9-7. SMS Anti-Spam log entries

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

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

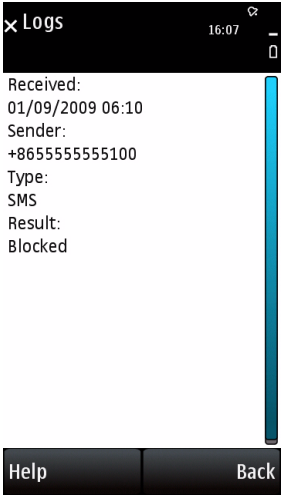

Figure 9-8. SMS Anti-Spam log entry details

WAP Push Log

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

Figure 9-9. WAP Push Log entries

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

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

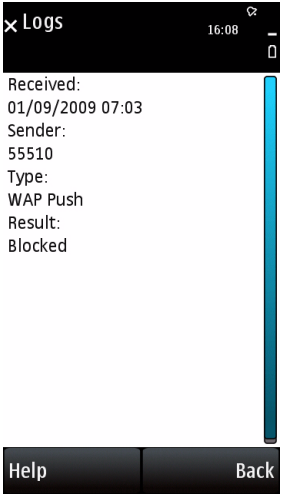

Figure 9-10. WAP Push log entry details

Viewing Logs

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

To view log entries:

1. Tap **Options > Logs** and then select the log type. *Figure 9-11* shows the log types in the **Logs** submenu.
2. In the log screen, tap the log entry you wish to view.

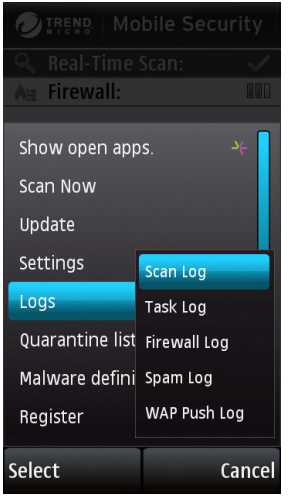

Figure 9-11. Event logs submenu

Deleting Logs

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

To clear a log:

1. Tap **Options > Logs** and then tap the log type.
2. Tap **Options > Clear log**.
3. Tap **Yes** on the confirmation prompt.

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

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* on page 10-2
- *Frequently Asked Questions (FAQ)* on page 10-6
- *Technical Support* on page 10-8
- *About TrendLabs* on page 10-12
- *About Trend Micro* on page 10-13

Troubleshooting

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

ISSUE	RECOMMENDED ACTION
The mobile device encountered a battery failure while installing Mobile Security. The installation process was stopped.	Ensure that the mobile device has adequate power and perform the installation process again.
The battery failed while uninstalling Mobile Security. Subsequent installation efforts would always fail.	Uninstallation did not complete. Use available tools designed for your mobile 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 mobile device. If you are approaching the device's maximum memory limit, consider deleting unnecessary files and applications.

ISSUE	RECOMMENDED ACTION
I cannot perform updates while the mobile device is connected to a host computer.	Verify the following: • Mobile Security is registered to the Mobile Security Management server successfully • The device's proxy settings are identical to the host computer's settings • The host computer is able to connect to the Mobile Security Management server • The Mobile Security component update option is enabled on your mobile device. If you cannot change Mobile Security policies on your mobile device, contact your network administrator.
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 policies.
I cannot receive WAP Push messages even when I choose to accept the messages.	Your mobile device or service may not support receiving WAP Push messages. Check your device's documentation or contact your service provider to find out whether you can receive WAP Push messages.

ISSUE	RECOMMENDED ACTION
A message pops up that requests to open a wireless connection.	This is normal if you have selected the **Connection alert** option in the **Update settings** screen. You can disable this option, but you will not be warned whenever Mobile Security opens a wireless connection to check for updates.
Mobile Security has been installed successfully. However, a security risk being copied could not be detected.	Verify that the Activation Code has not expired. When Mobile Security license on your mobile device is expired, component update is disabled. Out-of-date components on your mobile device may not detect the latest security risks. Trend Micro recommends opening the Mobile Security main screen after installation to ensure that all modules are loaded. Contact your system administrator for assistance.

ISSUE	RECOMMENDED ACTION
I cannot copy a file into the mobile device.	The file may be infected and is being blocked by Mobile Security. You can disable Real-time Scan, but this may compromise proactive security for your mobile 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.	Try restarting your mobile device. Mobile Security requires a restart after installation to load the firewall or the WAP Push Protection driver.

Frequently Asked Questions (FAQ)

Can I install Mobile Security on a storage card?

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

How long can I use Mobile Security and download program and the Malware Pattern updates?

You can check the expiration date of your license by selecting **Options > About** on the main screen.

Can I download malware pattern files to a storage card even though Mobile Security is installed directly on the mobile device?

No. The malware pattern files are downloaded and installed to the same location where you installed Mobile Security.

How often should I update Mobile Security program components?

Trend Micro recommends updating program components weekly.

Can Mobile Security scan compressed files?

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

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

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

Can I clean detected security risks?

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

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

Mobile Security allows each type of log a maximum of 16KB of memory.

Can I open infected/suspicious files on my mobile device?

With real-time scan enabled, Mobile Security will block the opening, copying, or moving of any detected security risks. You may disable real-time scan, but this may compromise proactive security for your mobile device.

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

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

Can a quarantined file be opened again?

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

How does Mobile Security match sender numbers to my SMS Anti-Spam filtering and WAP Push trusted lists?

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

Can I install Mobile Security with other security products?

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

Can I extend the license of my installation copy?

Yes. Contact your system administrator for assistance.

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, mobile device, and email, or visit us at:

http://www.trendmicro.com

Speeding up Support Calls

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 your mobile device
- Network type
- Computer and mobile device brand, model, and any additional hardware connected to your mobile device
- Amount of memory and free space on your mobile 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 anti-malware 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 malware**, you will be prompted to supply the following information:

- **Email—**the email address where you would like to receive a response from the anti-malware 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 infected/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 malware 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 anti-malware 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 malware pattern file updates and scan engine refinements.

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

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

About Trend Micro

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

Glossary

TERMINOLOGY	DEFINITION
ActiveUpdate	the technology that Trend Micro products use to properly download and install updates from Trend Micro servers
antimalware	technology designed to detect and handle malware and other malware
antispam	technology designed to filter unwanted content as it is received by a messaging application or platform
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

TERMINOLOGY	DEFINITION
event logs	logs containing the results of product functions
filtering	the process of distinguishing and handling unwanted content
firewall	an application or mobile device that controls access to ports to regulate network communication to and from a computer or mobile 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
infected/suspicious files	files that have been found to contain viruses and other malware
malware	a general term that refers to all kinds of malicious applications such as malware and Trojans

TERMINOLOGY	DEFINITION
virus	a kind of malware that can propagate by distributing copies of itself or by infecting other files or both
malware pattern	collection of malware code snippets that the scan engine uses as a basis for identifying malware
pattern	see *malware pattern*
PC Suite	application that allows computers to connect and communicate with a mobile device running Symbian OS. S60 is a platform running on of Symbian OS
port	the endpoint of a logical rather than physical network connection. Ports are numbered such that each number refers to a type of logical connection. For example, when a firewall blocks a certain port number, it is actually blocking a type of logical connection
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

TERMINOLOGY	DEFINITION
scan engine	the anti-malware 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 *malware 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 Anti-Malware Policies* on page 5-10)

TERMINOLOGY	DEFINITION
WAP	Wireless Application Protocol; this protocol is typically used to provide Web content to mobile devices, which often have limited network bandwidth, processing capabilities, and display space
WAP Push	automatic method of delivering content, such as applications and system policies, to mobile devices through the Wireless Application Protocol
WAP Push message	an SMS message that acts as a confirmation prompt prior to the delivery of WAP Push content

Index

A

action on infected/suspicious files 5-11
ActiveUpdate G-1
advanced settings 4-2
anti-malware G-1
  advanced settings 5-10
  log 9-2
anti-spam 7-1, G-1
approved list 7-2
automatic updates 4-3–4-4

B

blocked list 7-2
blocked SMS messages 7-11
blocked WAP Push messages 8-7
blocking unidentified senders 7-9
Bluetooth 1-2

C

card scan 5-3, 5-5, G-1
CDMA2000 G-1
common ports 6-2
compression layers 5-11

D

default policies 3-7
delete 5-5
deny access 5-5
DNS 6-5
DoS 1-2

E

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

F

FAQ 10-6
filtering G-2
firewall 1-2, 6-1, 6-8, G-2
  advanced settings 6-9
  default rules 6-5
  deleting rules 6-14
  enabling 6-7
  log 9-6
  predefined protection levels 6-2
  rule details 6-10
  rule list 6-13
  rules 6-2, 6-9
firewall rules G-2
firewalls 6-2

forced updates 4-3
FTP 6-5

G

getting started 3-1
GPRS G-2

H

handheld device requirements 2-4
host computer requirements 2-4
HTTP 6-5
HTTPS 6-5

I

IDS 6-16, G-2
infected/suspicious files 5-7
installation 2-5
Internet 4-2
intrusion detection system 6-16
IP address 6-9

K

Knowledge Base 10-9

M

main menu 3-6
main screen 3-4
malware G-2–G-3
malware pattern G-3
manual scan 5-3
manual updates 4-3, 4-5
mobile malware 1-2, 5-12
Mobile Security
  features 1-3
  overview 1-2
mobile threats 1-2, 5-12
move rule pointer 6-14

P

pattern G-3
PC Suite 2-4, G-3
POP3 6-5
ports 6-9, G-3
predefined protection levels 6-8

Q

quarantine 5-5
quarantined files 5-9

R

real-time scan 5-3, G-3
  default action 5-5
  enabling 5-4
registration 2-8

S

safe practices 1-2
scan G-3
scan engine G-4

scan log 9-2
scan results 5-6
  delete 5-7
  quarantine 5-7
scan types 5-3
scanning 3-11, 5-1
scheduled updates 4-3–4-4
security risks G-4
SIS files 5-11
SMS 1-2, G-4
SMS anti-spam
  adding senders 7-5
  deleting senders 7-8
  disabling 7-10
  editing sender information 7-8
  enabling 7-3
  filter types 7-2
  log 9-8
SMS filtering 7-1
SMTP 6-5
spam 1-2
Spam folder 7-11
spam log 9-8
Submission Wizard 10-11
submitting infected/suspicious files 10-11
subnet 6-9
supported handheld device models 2-4
SYN flood G-4
system requirements 2-4

T

task log 9-4
technical support 10-8
Telnet 6-5
Trend Micro 10-13
TrendLabs 10-12
troubleshooting 10-2
trusted senders list 8-4
  adding senders 8-4
  deleting senders 8-6
  modifying senders 8-5

U

uninstallation 2-10
unscannable files 5-7, G-4
update types 4-3
updating 3-11, 4-1
UPnP 6-5
user interface 3-7

W

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

Windows 2-4

Z

ZIP files 5-11