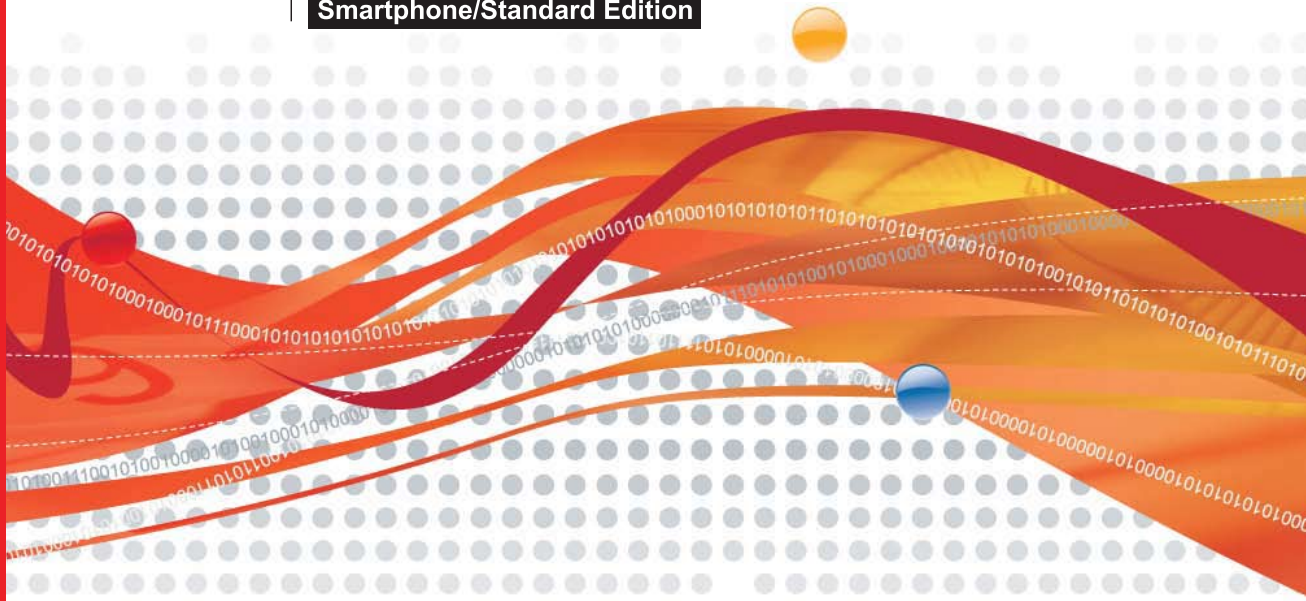
Trend Micro™ Mobile Security 5

for Microsoft™ Windows Mobile™ 5/6

Smartphone/Standard Edition



User's Guide

Release Date: March 2010

Document Part No.: TSEM53678/80528

The User's Guide for Trend Micro Mobile Security for Enterprise v5.5 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 mobile device. Read this chapter to understand how Mobile Security can protect your device.

This chapter covers the following topics:

Understanding Mobile Threats

With the standardization of platforms and their increasing connectivity, mobile devices are susceptible to an increasing number of 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 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 turned 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 allow Mobile Security to effectively block unwanted network communication (such as SMS messages and WAP push mails) to mobile devices. On Windows Mobile devices, the encryption module for Mobile Security provides logon password protection and data encryption for added security.

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, security policies, and program versions
- Logon authentication prevents anyone from accessing your mobile device

- Data encryption ensures data is secure whether it is stored on your mobile device or the inserted memory card
- Award-winning anti-malware scanning technology to scan for mobile 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 5.5

You can upgrade Mobile Security from version 5.0 or 5.1 to 5.5 on mobile devices without uninstalling the old version first. The setup program automatically uninstalls Mobile Security 5.0 or 5.1 before installing Mobile Security 5.5.

If your mobile device is using Mobile Security 2.0 or 3.0, you must uninstall the old version first before you can upgrade to version 5.5.

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 install Mobile Security manually on your mobile device.

This chapter covers the following topics:

Before Installing

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

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

- installation method
- initial power-on password (if the encryption module is enabled by your network administrator)
- registration information (if manual registration is required)

To use the encryption module on your Windows Mobile device, you must first:

Disable the password security or memory card encryption feature that comes with Windows Mobile on your mobile device. The encryption module will not work if the built-in password security or memory card encryption is enabled.

Also, remove any third-party password security program. You may be prompted to remove the program during the installation process.

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 or WAP Push message
- Using a memory card
- Executing the setup file (this method also requires 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 Message	• Installation SMS and WAP Push messages in the inbox on your mobile device • Initial power-on password

TABLE 2-1. Required information for manual installation

METHOD	REQUIRED INFORMATION
Memory Card	• A memory card with the Mobile Security setup file in the root folder • Initial power-on password
Executing Setup File	• Mobile Security setup file • A host computer with ActiveSync 4.2 (for Windows Mobile 5), 4.5 (for Windows Mobile 6), or above • Initial power-on password • Registration information (such as the server IP address and service port number)

System Requirements

Before installing and using Mobile Security, ensure that your mobile device meets the requirements.

TABLE 2-2. Operating system and mobile device memory requirements

OPERATING SYSTEM	MEMORY (MB)	STORAGE (MB)
Windows Mobile 5 Pocket PC/Pocket PC Phone	3	5.5
Windows Mobile 6 Classic/ Professional	3	5.5
Windows Mobile 5 Smartphone	3	5
Windows Mobile 6 Standard	3	5

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

To determine the Windows Mobile version running on your Smartphone:

1. Select **Start** > **Main Menu > Settings**.
2. Select **About** from the list.
3. On the **About** screen, verify the Windows Mobile version.

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 mobile device
- To update Mobile Security components and configuration through the computer's Internet connection

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

Using ActiveSync

You may need to use Microsoft ActiveSync (or Sync Center on Windows Vista) 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 the device to a computer with an active Internet connection.

To copy 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 2-3 shows the required ActiveSync settings for common tasks.

TABLE 2-3. Required ActiveSync settings

TASK	REQUIRED ACTIVESYNC SETTINGS
Copy installation file	Connect as a guest
Update components	Standard synchronization relationship; same proxy server settings on device and computer

ActiveSync displays the name of the device and automatically synchronizes data when in a standard synchronization relationship as shown in *Figure 2-1*.

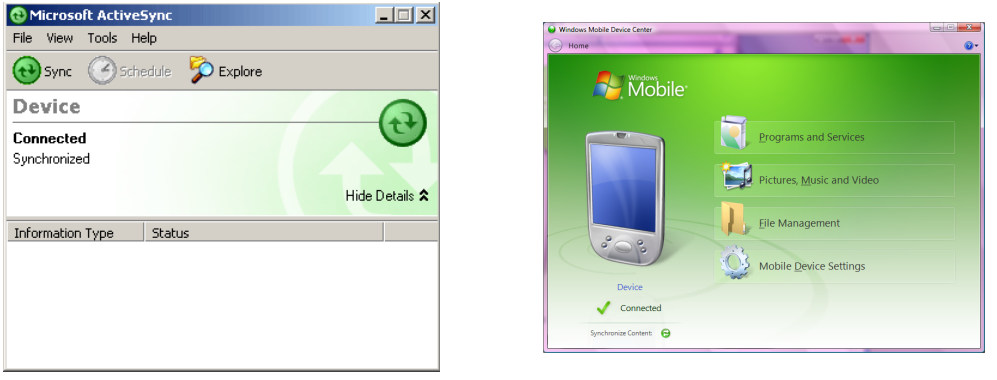


FIGURE 2-1. Microsoft ActiveSync and Sync Center connected in a standard synchronization relationship

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

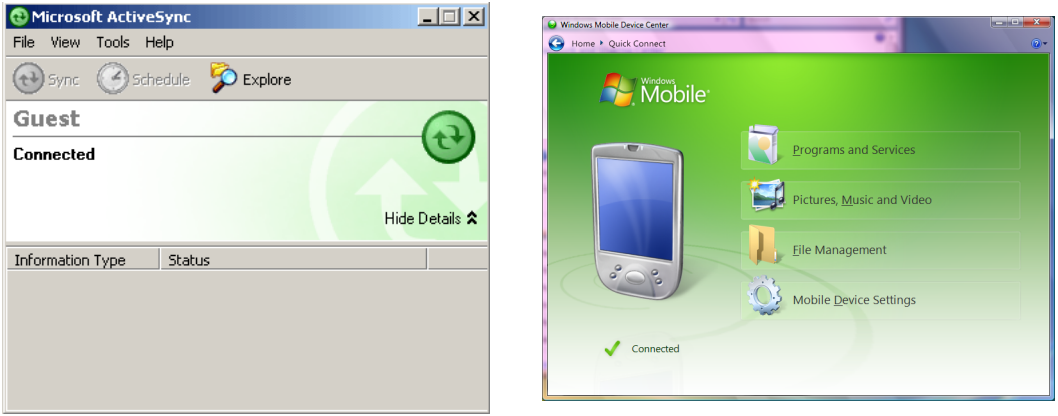


FIGURE 2-2. Microsoft ActiveSync and Sync Center with device connected as a guest

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

Installing Mobile Security

This section shows you how to manually install Mobile Security on your mobile device. After the installation is complete, Mobile Security is added to the **Start** menu.

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

To manually 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 device should have received SMS messages from the Mobile Security Management server.
   a. If your mobile device is able to process WAP Push messages, your mobile device will automatically download the Mobile Security setup package and install the product.
   b. If your mobile device does not support WAP Push messages, you need to open the SMS message and access the URL to download the Mobile Security setup package. When prompted, select the platform for your mobile device. After the file download is completed, your mobile device automatically installs Mobile Security.

Do not delete the registration SMS message from the inbox. Mobile Security 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. After the installation process is completed, your mobile device will automatically register to the Mobile Security Management server. After product registration is successful, you may be prompted to type initial password.

To manually install Mobile Security using a memory card:

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.

Insert the memory card into your mobile device. Setup automatically installs Mobile Security. After the installation process is completed, your mobile device will automatically register to the Mobile Security Management server.

After product registration is successful, you may be prompted to type initial password.

To manually install Mobile Security by executing the setup file:

1. Copy the setup file MobileSecurity_SP.cab to your mobile 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, navigate to the location of the setup file.
3. Open the setup file to start installing Mobile Security. After the installation is complete, Mobile Security is added to the **Start** menu.
4. Manually register your device to the Mobile Security Management server (refer to *Manual Registration* on page 2-12 for more information). After product registration is successful, you may be prompted to type initial password.

Manual Registration

Register your mobile device to the Mobile Security Management server to obtain the licenses for Mobile Security and the encryption module on your mobile device. Depending on the installation method used, your mobile device may automatically register to the Mobile Security Management server after installing Mobile Security.

If your mobile device is not registered to the Mobile Security Management server, the **Register** screen displays after you log on for the first time. 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 device to the Mobile Security Management server at this time, you can still use Mobile Security on your mobile device with an evaluation license of thirty days. The evaluation license allows you to use all product features except component updates and encryption module.

To register your device to the Mobile Security Management server:

1. Configure the fields in the **Register** screen (**Menu > Register**):
   - **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.
2. Tap **Register**. A pop-up screen displays prompting you to confirm. Select **OK** to continue. The registration process may take several minutes depending on your network connection.
3. After the registration is completed successfully, the main Mobile Security screen displays.

Using Encryption

The encryption module provides the power-on password and encryption features on your mobile device. Activation of the encryption module is automatic on your mobile device if all of the following requirements are met:

- Mobile Security is installed

- Mobile Security has successfully registered to the Mobile Security Management server
- the encryption license is included in the product license
- the encryption module is enabled by the server administrator

After registering to Mobile Security Management server, mobile device agent will get the encryption policy from the server. You will be prompted to type the power on password. You may also be prompted to change the password and set the response in case you forget the password, which depends on your administrator's encryption policy. After that, the encryption module will start applying the encryption policy.

Initial Logon

After applying the encryption policy on your mobile device, you need to type the initial power-on password in the **Password** screen to log on. After the initial logon, you may be prompted to change the power-on password and/or select a reset password question and set the answer.

If you do not have the initial power-on password, do not attempt to log on. Contact your network administration for information.

To log on to your device for the first time:

1. In the **Password** screen, type the initial logon password provided by your network administrator.
2. Tap **OK**.

Changing Password after Initial Logon

Depending on your network security policy, you may be required to change the initial power-on password after the first logon.

To change the password after the initial logon:

1. After the initial logon, a screen displays prompting you to change the password. Type a new power-on password in the **Password** field.
2. Type the new power-on password again in the **Confirm** field.
3. Tap **Done**. A screen displays to indicate whether the password change is successful.

After setting the power-on password, you may need to type the same password on a host computer before the computer can connect to your device using ActiveSync.

Setting Forgotten Password Question and Answer

You may be prompted to specify the forgotten password question and answer. If you have forgotten the power-on password, you can still unlock your device by typing the correct answer to the selected question.

To set the forgotten password question and answer after initial logon:

1. After the initial logon, a screen displays prompting you to select a question. Scroll through the list of questions to select a question.
2. Set the answer to the question you have selected. Type the answer in the **Password** fields.
3. Tap **Done**. A screen displays indicating that the forgotten password question and answer are set successfully. Close the pop-up screen to log on to your mobile device.

Uninstallation

You can uninstall the Mobile Device Agent on the device or through a host computer.

To uninstall directly on the device:

1. Select **Start > Main Menu > Settings**.
2. Select **Remove Programs**.
3. Select **Trend Micro Mobile Security**.
4. Select **Menu** > **Remove**.
5. When Windows Mobile prompts you for confirmation, select **Yes**.

6. If prompted, type the uninstall password and select **OK** to continue.

You can contact your system administrator to provide the password if needed.

After a cancelled or failed uninstallation, be sure to select "No" from the dialog:

Trend Micro Mobile Security was not completely removed. Do you want to remove it from the list of installed programs? Selecting "Yes" may unexpectedly complete the uninstallation.

7. 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.
8. If the encryption is enabled on your mobile device, it will prompt for power-on password. Enter your power-on password. After you enter the correct password, it will start decrypting the data on your mobile device.

9. After the decryption is completed, the system starts removing Mobile Security. Upon completion , the successfull message will be displayed on the screen.

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, select **Tools** > **Add/Remove Programs**.
4. In the programs list, select **Trend Micro Mobile Security** and select **Remove**.
5. When ActiveSync prompts for your confirmation, select **OK**.
6. If prompted, type the uninstall password and select **OK** to continue.
7. 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.
8. If the encryption is enabled on your mobile device, it will prompt for power-on password. Enter your power-on password. After you enter the correct password, it will start decrypting the data on your mobile device.
9. After the decryption is completed, the system starts removing Mobile Security. Upon completion , the successfull message will be displayed on the screen.

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 policies.

This chapter covers the following topics:

- *The About Screen* on page 3-11
- *Owner Information* on page 3-7
- *Product License* on page 3-11
- *Reviewing Default Protection Policies* on page 3-12
- *Updating Anti-Malware Components* on page 3-15
- *Scanning for Malware* on page 3-16

- *Reviewing Default Protection Policies* on page 3-12
- *Updating Anti-Malware Components* on page 3-15
- *Scanning for Malware* on page 3-16

Power-on Password

After installing Mobile Security and enabling the encryption module, you need to set the logon password (also known as the power-on password) for your mobile device. The power-on password prevents unauthorized access to your mobile device.

Your network administrator should provide you with the information related to password policy.

- Types of characters allowed for the password. For example, the password can only contain numbers or both alphabetic characters and numbers.

- Password complexity if alphanumeric characters are allowed for your password. For example, whether you need to type a mix of upper case and lower case characters or whether you need to type at least one non-alphanumeric character.
- The time before your current password expires. You will need to set a new password after the expiration date.
- The number of times you can type an incorrect password.

If you type the incorrect password too many times, your mobile device may:

- **Restart and require you to type the power-on password**
- **Require the administrator password to unlock the mobile device and reset the power-on password**
- **Hard reset the mobile device to revert to factory default settings and clear all the data on the mobile device**
- **Hard reset the mobile device to revert to factory default settings and clear all the data on the mobile device and the storage card**

Changing the Password

You may need to change the password after the current password expires.

To change the power-on password:

1. In the **Password** screen, select **Menu > Change Password**.
2. Type your current password in the **Old Password** field.
3. Type the new password in the **New Password** field.
4. Type the same password in the **Confirm new Password** field for confirmation.
5. Select **Done** to save the changes. When the password change is successful, a message displays.

After changing the password, use the new password to log on the device.

Resetting the Password

If you have forgotten your password, you may unlock your device and reset the password using one of the following methods:

- Type the answer to the reset password question you selected
- Have your administrator remotely unlock your device and provide you with a response code to reset the password

To reset the password by answering the reset password question:

1. In the **Password** screen, select **Menu > Forgot Password**. The reset password question displays.
2. Type your answer and select **Done**.
3. You are prompted to set a new password. Type the new password in the **Password** and **Confirm** fields.
4. Select **Done**. After the password reset is successful, you can access your device.

To remotely unlock your mobile device:

1. In the **Password** screen, select **Menu > Remote Unlock**.
2. Your device automatically generates a pass code. You can select **Change** to generate a new code.
3. Give this pass code to your network administrator. Do not close the **Remote Unlock** screen or select any button.
4. When instructed by your network administrator, select **Next**.
5. Type the response code and select **OK**.
6. If the password reset is successful, you are prompted to set a new password. Type the new password in the **Password** and **Confirm** fields.
7. Select **Done**. After the password reset is successful, you can access your device.

Locking Mobile Devices

Your device automatically enters the secure mode after a period of inactivity. That is, the mobile device logs you out and displays the **Power-On Password** screen. The inactivity timeout period varies depending on your company policy. Consult your network administrator for this information.

To manually lock your mobile device:

1. Select **Start** > **Main Menu** > **Settings** > **Security**.
2. Select **Device Lock**
3. The **Power-On Password** screen appears.

When your mobile device is locked, you can still make emergency calls but you cannot access files or programs.

Unlocking Mobile Devices

To unlock your mobile device, type the **Power-On Password** and select **OK**.

If you type the incorrect password too many times, your mobile device may:

- **Restart and require you to type the Power-On Password**
- **Require the administrator password to unlock the device and reset the Power-On Password**
- **Hard reset the mobile device to revert to factory default settings and clear all the data on the mobile device**
- **Hard reset the mobile device to revert to factory default settings and clear all the data on the mobile device and the storage card**

Owner Information

You can set the owner information on your mobile device and view that information when the mobile device is locked.

To set owner information on your mobile device:

1. **Start** > **Main Menu** > **Settings** >
2. Select **Owner Information**.
3. On the **Owner Information** screen, type the owner information in the associated fields.

4. Select **Done** to save the information and exit.

To view owner's information when the mobile device is locked:

1. Select **Menu > Owner**. The owner information screen appears.

Data Encryption

To ensure that data is protected on your mobile device, the encryption module in Mobile Security encrypts files and/or data on your device. Depending on your company policy, data stored in memory cards may also be encrypted to prevent anyone outside your company from opening encrypted files in your memory card. Consult your network administrator for more information.

For example, if you use your mobile device to open and save a file on a memory card while the memory card data encryption is enabled, the file is encrypted. However, if you only view a file on the memory card from your mobile device without any modification, the file is not encrypted.

When the encryption module is disabled by your administrator or the evaluation license expires, Mobile Security automatically decrypts all encrypted files or data on your mobile device and the inserted memory card.

Mobile Security encrypt files according to file extensions that are defined by the administrator. Only trusted applications that administrator set can handle encrypted files. If you are facing problems with third-party applications, contact your administrator for assistance.

Understanding the Mobile Security Interface

Mobile Security has an easy-to-use interface that enables access to the various product features. The main interface includes the following:

- *Main Screen*
- *Menu Items*

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	Update the product

Figure 3-1. Main screen

Menu Items

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

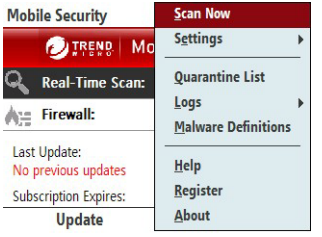


Figure 3-2. Main screen menu

TABLE 3-2. Main screen menu items

MENU ITEM	ACTION
Scan Now	Scan your device for malware
Settings	Access product options
Quarantine List	Access quarantined files
Logs	View event logs
Malware Definitions	View definitions of known mobile malware
Register	Register the product
About	View the About screen

Product License

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

If Mobile Security is not registered to the Mobile Security Management server and the evaluation license expires, all Mobile Security features are disabled on your mobile device.

If the full license for Mobile Security expires, you can still use the encryption, firewall and the malware scan features. However, malware scans may use out-of-date anti-malware components and therefore may not detect the latest security risks.

The About Screen

To view the product license information, tap **Menu > About** to display the About screen. You can see the expiry dates for the standard license and encryption license.

The standard license is for the anti-malware and firewall features in Mobile Security while the advanced license activates the encryption module for logon authentication and data encryption.

Reviewing Default Protection Policies

After installation, Mobile Security is ready to protect your device against mobile malware and other threats.

Your network administrator may not allow you to change Mobile Security 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.

Review the default protection policies shown in *Table 3-3* to assess whether you want to modify them.

TABLE 3-3. Default protection policies

FEATURE	DEFAULT POLICY	RESULTING ACTION
Real-time scan	Enabled	Product scans files that are being accessed.
Real-time action	Quarantine	Product encrypts and moves infected/suspicious files.
Card scan	Disabled	Product does not scan memory cards automatically when inserted.

TABLE 3-3. Default protection policies

FEATURE	DEFAULT POLICY	RESULTING ACTION
File types to scan	All	Product scans all files for malware.
CAB/ZIP layers to scan	3 (maximum)	Product extracts compressed files (CAB/ZIP) 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.
Wireless connection alert	Enabled	Product displays a confirmation message before opening a GPRS or other wireless connections to access the Internet.
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.

TABLE 3-3. Default protection policies

FEATURE	DEFAULT POLICY	RESULTING ACTION
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.
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.
SMS anti-spam	Disabled	Product does not filter SMS messages and allows all messages to reach the message inbox. You can enable or disable this feature on your mobile device.
WAP Push protection	Disabled	Product does not filter WAP Push messages and allows all messages to reach the 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 malware, update Mobile Security after installation.

To update Mobile Security:

1. Ensure that your mobile device can connect to the Mobile Security Management server.
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 Anti-Malware Components* on page 4-1.

If your mobile device is not registered to the Mobile Security Management server, the update feature is disabled.

Scanning for Malware

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

If a malware is detected on your mobile device, Mobile Security generates and sends a security risk log to the Mobile Security Management server. A screen may display prompting you to allow your mobile device to connect to the Mobile Security Management server.

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, update the anti-malware components regularly.

This chapter covers the following topics:

Connecting to the Mobile Security Management Server

To update components for Mobile Security, your mobile device must connect to the Mobile Security Management server. If required, you can type the IP address and port number of the Mobile Security Management server in the **Register** screen (see *Manual Registration* on page 2-12).

Types of Updates

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.
Automatic	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	Runs 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 Mobile Security Management server.

Automatic and Force Updates

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

To configure automatic and force update intervals:

1. Select **Menu > Settings > Update**. The **Update** screen opens as shown in *Figure 4-1*.
2. On the **Update** 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.

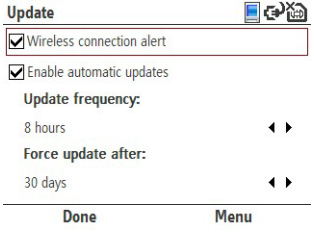


Figure 4-1. Update Options screen

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 Mobile Security to display a message before opening a wireless connection, select **Wireless connection alert** on the **Update** screen.

Manual Update

To perform a manual update:

1. Ensure that your mobile device is 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 Malware

Trend Micro Mobile Security scans your device for mobile malware. Read this chapter to understand the anti-malware features of Mobile Security.

This chapter covers the following topics:

• *Information on 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 device for malware. To run a manual scan, select **Menu > Scan** on the main screen.

The scan results screen displays a list of any infected/suspicious 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 device access them. This scan prevents device users from inadvertently executing malware.

Enabling Real-time Scan

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

To enable real-time scan:

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

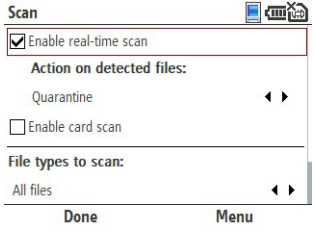


Figure 5-1. Scan Options screen

To disable real-time scan, clear **Enable real-time scan** in the **Scan Options** screen. If you disable real-time scan, proactive protection is unavailable on your mobile device.

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 feature is disabled by default. Enable card scan to automatically check memory cards for malware. When card scan is enabled and a memory card is inserted into your device, Mobile Security automatically starts malware scanning.

To enable card scan:

1. Select **Menu > Settings > Scan** 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 infected/suspicious and unscannable files as shown in *Figure 5-2*. You can either quarantine or delete these files.

Scan result items can either be infected/suspicious files or unscannable files as explained in *Table 5-2*.

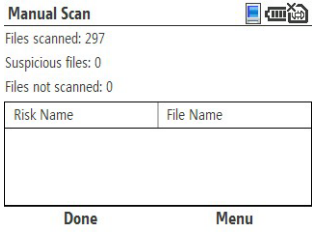


Figure 5-2. Scan results screen

TABLE 5-2. Scan results items

SCAN RESULT ITEM	DESCRIPTION
Suspicious files	Files found to contain malware

TABLE 5-2. Scan results items

SCAN RESULT ITEM	DESCRIPTION
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

To view details on a suspicious 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 Anti-Malware Policies* on page 5-9.

Handling Infected/Suspicious or Unscannable Files

If you exit the scan results screen without quarantining or deleting suspicious or unscannable files, these files stay in your device and cause damage to other files or affect the operation of your device.

To delete or quarantine infected/suspicious or unscannable files:

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

To quarantine or delete all infected/suspicious 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.

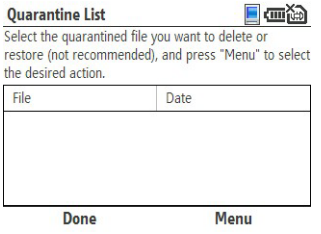


Figure 5-3. Quarantine List screen

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 infected/suspicious files after restoring them.

Advanced Anti-Malware Policies

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.

TABLE 5-1. Options for file types to scan

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

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 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 Advanced Scan Policies

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

To configure advanced scan policies:

1. From the main menu, select **Menu > Settings > Scan**.
2. Under **File types to scan**, select the types of files to scan for malware. For more information on the file type options, see *Table 5-1*.

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 Malware

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

To view additional details on a malware,

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

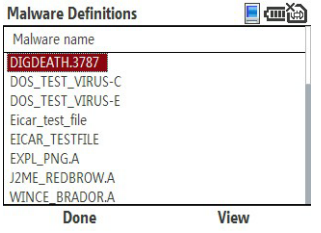


Figure 5-4. Malware Definitions screen

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 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 provides 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.

TABLE 6-1. Predefined protection levels

PROTECTION LEVEL	MODE	DESCRIPTION
Low	Open	All inbound and outbound traffic is allowed.

TABLE 6-1. Predefined protection levels

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

Since 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*.

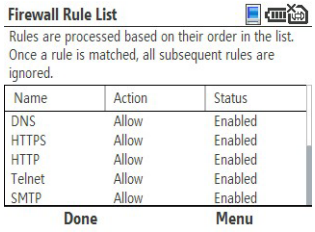


Figure 6-1. Firewall Rule List screen

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.

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

TABLE 6-2. Default firewall rules

RULE	PORT	COMMON USAGE	DEFAULT FIREWALL POLICY
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. Select **Menu > Settings > Firewall** on the main screen. The **Firewall** screen opens as shown in *Figure 6-2*.
2. Select **Enable firewall**.
3. Select **Done**.

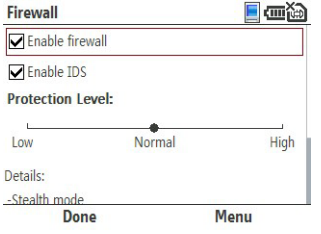


Figure 6-2. Firewall Options screen

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 6-3*.

To configure your firewall protection level:

1. Select **Menu > Settings > Firewall** 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 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, 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 > Settings > Firewall** 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*.

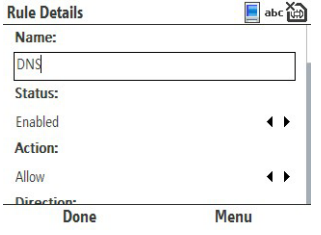


Figure 6-3. Rule Details screen

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*.

TABLE 6-3. Rule details screen items

ITEM	OPTIONS	DEFINITION
Status	• Enabled • Disabled	Enables or disables the rule
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

TABLE 6-3. Rule details screen items

ITEM	OPTIONS	DEFINITION
Protocol	• All • TCP/UDP • TCP • UDP • ICMP	Determines the network protocol to which this rule applies
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.

TABLE 6-3. Rule details screen items

ITEM	OPTIONS	DEFINITION
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.

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 > Settings > Firewall** 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**.

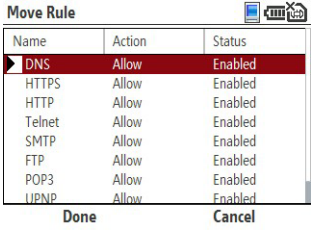


Figure 6-4. Moving a firewall rule

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.

Deleting Firewall Rules

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

To delete a firewall rule:

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

The IDS will block only SYN flood attacks.

Chapter 7

Filtering SMS Messages

On a mobile device with the phone feature, 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 7-8.

SMS Anti-Spam Configuration

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

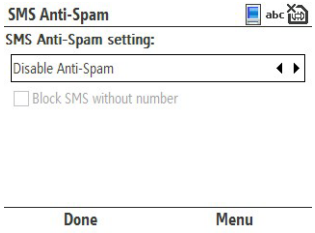


Figure 7-1. SMS Anti-Spam screen

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 > Settings > SMS Anti-Spam** on the main screen.
2. Under **SMS Anti-Spam setting**, select either **Enable approved list** or **Enable blocked list**.

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 mobile device's contact list

To manually enter sender details:

1. Select **Menu > Settings > 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**.
5. The **Add Sender** screen opens as shown in *Figure 7-3*.
6. Type the name and number of the sender.
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 > Settings > SMS Anti-Spam** on the main screen.
2. Ensure that an anti-spam list is enabled.

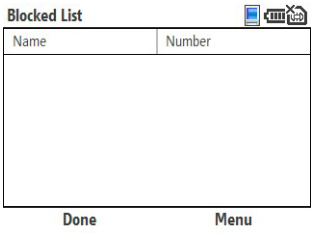


Figure 7-2. SMS anti-spam blocked list

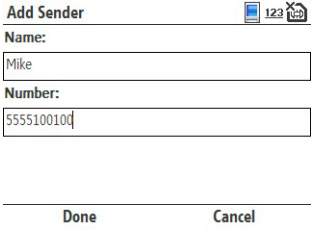


Figure 7-3. Add Sender screen

3. Select **Menu > Set Approved/Blocked List**. Mobile Security displays the current list entries as shown in *Figure 7-4*.
4. Select **Menu > Import.** Mobile Security lists all contacts as shown in *Figure 7-5*.
5. Select the contacts to import under **Select contacts** and then select **Import**.

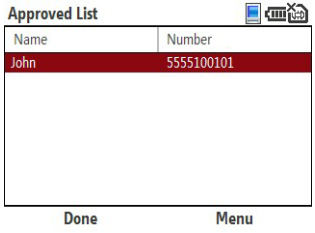


Figure 7-4. SMS anti-spam approved list

6. Verify that your contacts have been imported as shown in *Figure 7-5*.
7. Select **Done** to save the changes and return to the **Anti-Spam Options** screen.

Figure 7-5. Import Wizard scree

Editing the 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 > Settings > SMS Anti-Spam** on the main screen.
2. Ensure that an anti-spam list is enabled.

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

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

6. Select Done to save the changes and return to the SMS Anti-Spam setting 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 > Settings > 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 7-6*
4. Select **Done**.

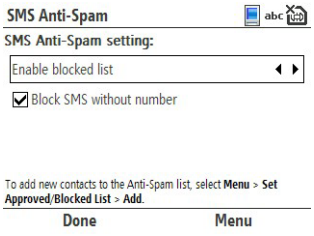


Figure 7-6. SMS Anti-Spam screen

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 policies do not block messages that you want to receive. See *Handling Blocked SMS Messages.* on page 7-8.

Disabling SMS Anti-Spam Filtering

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

To disable all SMS filtering:

1. Select **Menu > Settings > SMS Anti-Spam** on the main screen.
2. Under **SMS Anti-Spam setting**, 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 7-7*). You can handle these messages as you would handle other messages in your Inbox folder

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

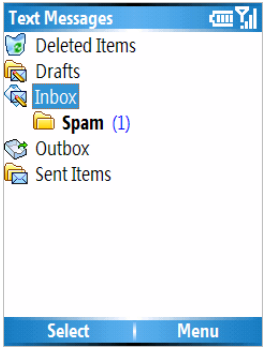


Figure 7-7. Mobile Security Spam folder

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 mobile devices automatically. It may be used to deliver mobile-related content such as ringtones, news, email, and 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 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.

The WAP Push Protection menu option is not available on mobile devices without the phone feature.

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 > Settings > 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**.

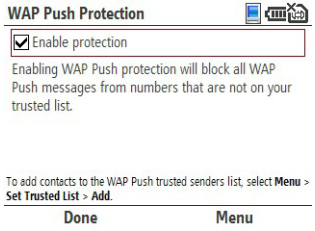


Figure 8-1. WAP Push Protection options screen

Managing the WAP Push Trusted Senders List

Mobile Security will automatically allow messages from senders on your 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 > Settings > 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 **Menu > Add**. The **Add Sender** screen opens.
5. Type the name and number of the sender.
6. Select **Done**.

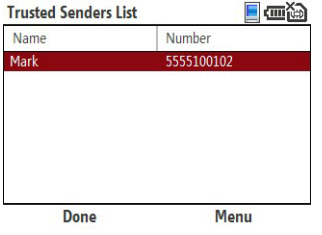


Figure 8-2. Trusted Senders List screen

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 > Settings > 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.
8.

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**.

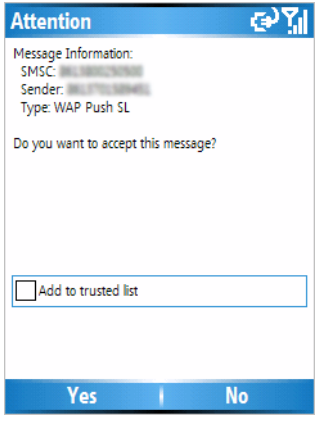


Figure 8-3. WAP Push alert message

Chapter 9

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.

ISSUE	RECOMMENDED ACTION
The encryption module does not work on my mobile device.	First verify the following: • Mobile Security is registered to the Mobile Security Management server successfully • License for Mobile Security includes the encryption module. Check with your network administrator for this information. • The built-in password security feature is disabled in Windows Mobile. • You have uninstalled any third-party encryption software on your device. • The encryption module is enabled by your network administrator. Then, reinstall Mobile Security on your device.
After Mobile Security is registered to the Mobile Security Management server successfully, I cannot configure Mobile Security policies on my mobile device.	Your network administrator may have disabled the option that allows you to customize Mobile Security policies on your device. Contact your network administrator for more information.

ISSUE	RECOMMENDED ACTION
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: • 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 device. If you cannot change Mobile Security policies on your device, contact your network administrator.

ISSUE	RECOMMENDED ACTION
I cannot perform updates using GPRS.	Verify the following: • Mobile Security is registered to the Mobile Security Management server successfully • Your device can connect 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. • Contact your network administrator to check that the server is configured properly for public access
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 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.

ISSUE	RECOMMENDED ACTION
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.
Mobile Security has been installed successfully. However, a security risk being copied could not be detected.	Contact your network administrator to check that license for Mobile Security has not expired.
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 this may compromise proactive security for your device
I cannot access the Internet or other network resources.	Check your firewall policies. 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.

ISSUE	RECOMMENDED ACTION
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.
Default password cannot be accepted.	Try restarting your device. If the problem persists, this is an indication that the policy was not applied. Try using the previous default password to log on.
My files are encrypted on the storage card, but Mobile Security was uninstalled. I cannot decrypt my files.	Check with your administrator. He/she can recover your files.
My files are encrypted on the storage card, but the device was lost. I want to decrypt my files.	Check with your administrator. He/she can recover your files.

ISSUE	RECOMMENDED ACTION
Whenever I try to quarantine files, the operation fails. While quarantining files, Mobile Security always prompt dialog saying "Unable to quarantine the file '%s'. The file may be read-only, no longer available, too large, or in use by another application. Close all applications and try again."	This occurs if too many files are in the quarantine directory. The operating system can store approximately only 1000 files in each directory. Try deleting few files in the quarantine folder before retrying.
My Dell X51v does not restart after Mobile Security requests for a restart.	On Dell X51v devices, there is a conflict between the operating system and the WiFi module. If a WiFi connection is open, this could occur. Solutions include disconnecting the WiFi module before restarting or manually removing the battery, reinserting the battery, and then powering on the device.
I have uninstalled Mobile Security but a few DLL files are still on my mobile device.	In some cases, the Mobile Security DLL files could be in use by other applications and cannot be deleted during uninstall. Ensure you restart the device to uninstall all components when prompted

ISSUE	RECOMMENDED ACTION
If Bluetooth feature is disabled, i-mate SP5 and Qtek 8300 devices tend to hang during the following sequence of events: 1. Turn off Bluetooth 2. Turn on Bluetooth 3. Turn on WiFi	Avoid this sequence of events. Try switching on WiFi before the Bluetooth module.
I have upgraded Mobile Security from version 5.0/5.1 to 5.5, and the encryption feature does not work on my mobile device.	The mobile device has not downloaded the encryption policy from the server. Perform an update on the mobile device to get the new encryption policy.
I have upgraded Mobile Security from version 5.0/5.1 to 5.5 on my mobile device, but the old encryption module fails to get uninstalled.	This could occour if the mobile device reboots before Mobile Security uninstalls old encryption module. To manually uninstall the encryption module, select **Settings > System > Remove Programs > Trend Micro Encryption Component**. The old admin password is required for this uninstallation. After completing the uninstallation, perform an update on the mobile device to get the new encryption policy.

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.

Certain features that were previously available are unavailable now. Why?

Your administrator might have disabled the availability of certain features. Contact your administrator before contacting support.

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. You may be prompted to uninstall these software products before you can install Mobile Security on your mobile device.

Can I download the Malware Pattern to a storage card even though Mobile Security is installed directly on the device?

No. The Malware Pattern is 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. Your network administrator may have already set up a scheduled update on your device.

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 malware and security risks.

Can I clean infected/suspicious 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 infected/suspicious files on my device?

No. With real-time scan enabled, Mobile Security will block the opening, copying, or moving of any suspicious security risks. You may disable real-time scan, but this may compromise proactive security for 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 does not filter both inbound and outbound network traffic that passes through an ActiveSync connection.

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 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 host computer and device
- 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 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 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.also call the following toll-free telephone number: (877) TRENDAV, or 877-873-6328.

About TrendLabs

TrendLabs[SM] 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 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 anti-malware 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.

Chapter 10

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

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 10-1*) every time it detects malware or an unscannable file.

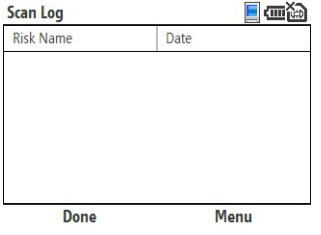


Figure 10-1. Scan log entries

Each scan log entry (shown in *Figure 10-2*) contains the following information:

- **Date & time**—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 or deleted
- **Result**—whether the action was successfully completed

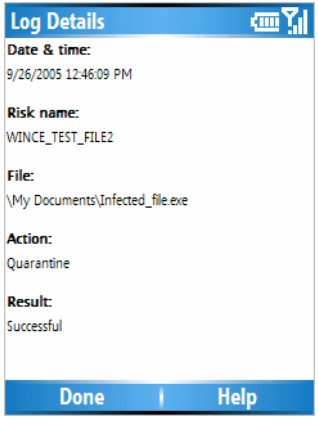


Figure 10-2. Scan log details

Task Log

Mobile Security generates an entry in the task log (shown in *Figure 10-3*) every time it runs a manual scan, a card scan, or an update.

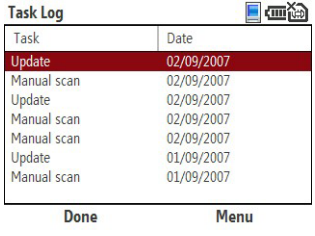


Figure 10-3. Task log entries

The following describes the information in a task log entry (shown in *Figure 10-4*):

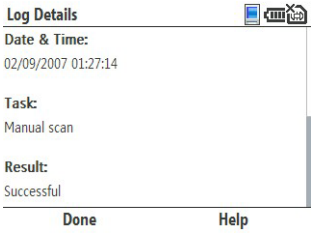


Figure 10-4. Task log details

- **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 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)

Firewall Log

Mobile Security generates an entry in the firewall log (shown in *Figure 10-5*) when one of the following occurs:

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

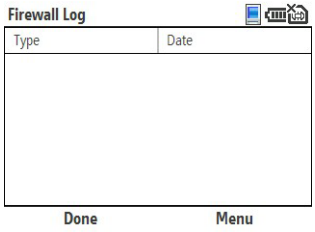


Figure 10-5. Firewall log entries

Each firewall log entry (shown in *Figure 10-6*) 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

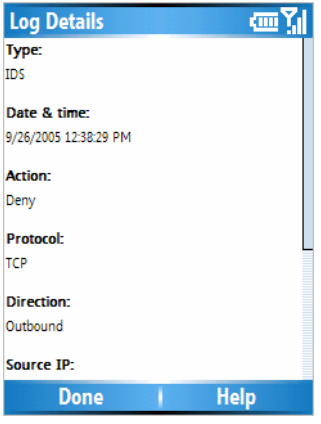


Figure 10-6. Firewall log details

Spam Log

Mobile Security generates an entry in the spam log (shown in *Figure 10-7*) every time it blocks an SMS message.

The Spam Log menu option is not available on mobile devices without the phone feature.

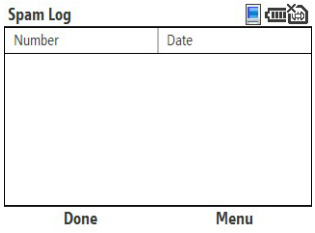


Figure 10-7. Spam log entries

Each spam log entry (shown in *Figure 10-8*) contains the following information:

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

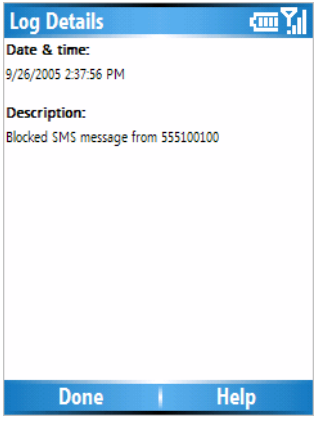


Figure 10-8. Spam log details

WAP Push Log

Mobile Security generates an entry in the WAP Push log (shown in *Figure 10-9*) every time it blocks a WAP Push message.

The WAP Push Log menu option is not available on mobile devices without the phone feature.

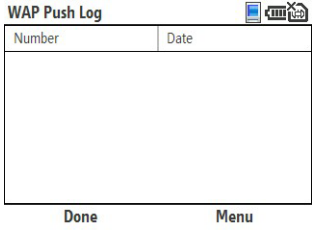


Figure 10-9. WAP Push log entries

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

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

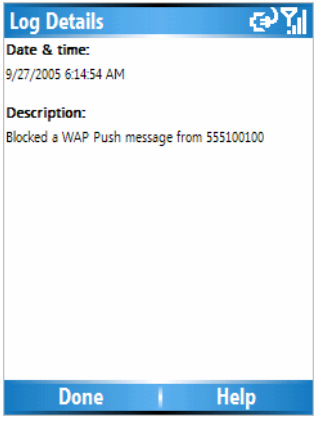


Figure 10-10. WAP Push log

Viewing Logs

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

To view log entries:

1. Select **Menu > Logs** and then select the log type. *Figure 10-11* shows the log types in the **Logs** submenu.
2. In the log screen, select the log entry you wish to view.

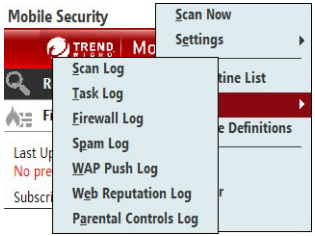


Figure 10-11. Event logs

Deleting Logs

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

To clear a log:

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

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

Glossary

TERMINOLOGY	DEFINITION
ActiveSync	an application that allows a Windows-based computer to connect and communicate with a mobile device running Windows Mobile.
ActiveUpdate	the technology that Trend Micro products use to properly download and install updates from Trend Micro servers.
anti-malware	technology designed to detect and handle malware.
anti-spam	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 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
data encryption	the process that converts data into non-readable format
detected files	files that have been found to contain malware.
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.

TERMINOLOGY	DEFINITION
pattern	see *malware 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.
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 malware.
scan engine	the anti-malware component that determines whether a file is a 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.

TERMINOLOGY	DEFINITION
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 5-9).
malware pattern	collection of malware code snippets that the scan engine uses as a basis for identifying malware.
virus	a kind of malware that can propagate by distributing copies of itself or by infecting other files or both.
WAP	Wireless Application Protocol; this protocol is typically used to provide Web content to 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.

TERMINOLOGY	DEFINITION
WAP Push message	an SMS message that displays as a confirmation prompt prior to the delivery of WAP Push content.

Index

S

T

U

W

Z