Trend Micro™ Mobile Security 3.0 Deployment Guide

April 2007

Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014
T 800.228.5651 / 408.257.1500
F 408.257.2003
www.trendmicro.com

ENTERPRISE TECHNICAL MARKETING

Contents

1. About this Deployment Guide

This *Deployment Guide* assists enterprise administrators in deploying and managing Trend Micro Mobile Security 3.0 using third-party device management (DM) frameworks such as Nokia™ Intellisync™, Sybase™ iAnywhere Afaria™, and Odyssey Software™ Athena™. This document discusses approaches typically supported by these DM frameworks. Note, however, that Trend Micro support is limited to the use of Trend Micro Mobile Security. For support with the third-party applications, contact their corresponding vendors.

This document specifically covers the following:

- Deploying Trend Micro Mobile Security using the silent install function
- Updating the scan engine and pattern
- Configuring application settings

Note: This Deployment Guide applies only to Trend Micro Mobile Security version 3.0. It does not apply to other versions of Trend Micro Mobile Security.

For the latest information about Trend Micro Mobile Security, including device support and the latest builds, visit www.trendmicro.com/mobilesecurity.

2. Deploying Trend Micro Mobile Security for Windows Mobile™ 5.0

2.1. System Requirements

To silently install and manage Trend Micro Mobile Security, the Windows Mobile device:

- Must be connected to a host computer with Microsoft™ ActiveSync™ 4.2
- Must have a copy of the installation file in the root folder; the name of the installation file is `MobileSecurity_PPC.cab` for the Pocket PC version and `MobileSecurity_SP.cab` for the Smartphone version.

By default, the file `wceload.exe` is in the `Windows` folder of Windows Mobile 5.0 devices. Ensure that this file has not been moved or deleted.

Note: You cannot run a silent installation through the Web or using WAP Push.

2.2. Installation

To install Trend Micro Mobile Security silently to a Windows Mobile device:

1. Install ActiveSync 4.2 to the host computer.
2. Copy the installation file, `MobileSecurity_PPC.cab` or `MobileSecurity_SP.cab`, to the root folder of the device.

   Tip: You can use a logon script to deploy ActiveSync 4.2 to the host computer and copy the installation file to the device. The logon script can automatically install ActiveSync or copy the installation file when users log on to your Active Directory domain.

3. To install Trend Micro Mobile Security, deploy the following command to the device:

   ```
   \Windows\wceload.exe \<name of installation file > /silent
   ```

   Note: `<name of installation file>` is either `MobileSecurity_PPC.cab` or `MobileSecurity_SP.cab`.

4. To set an Activation Code, deploy the following command to the device:

   ```
   \Program Files\Trend Micro\Mobile Security\3.0\TmDMAgent.exe /o ActiveCode=#
   ```

   Note: Replace the # with the Activation Code from Trend Micro.

3. Deploying Trend Micro Mobile Security for Symbian OS™/S60 3rd Edition

3.1. System Requirements

To silently install and manage Trend Micro Mobile Security, the S60 device:

- Must be connected to a host computer.
- Must have a copy of `MobileSecurity.sis`

Note: To run a silent installation, your device management (DM) framework must support silently installing SIS packages.

3.2. Installation

To install Trend Micro Mobile Security silently to an S60 device:

1. Copy `MobileSecurity.sis` to the device.
2. Use your DM framework to install the package silently.
3. To set an Activation Code, deploy the following command to the device:

   ```
   C:\sys\bin\TmDMAgent.exe /o ActiveCode=#
   ```

   Note: Replace the # with the Activation Code from Trend Micro.

4. Configuring Trend Micro Mobile Security

4.1. Understanding the Device Management Agent

The Device Management Agent `TmDMAgent.exe` enables remote management of Trend Micro Mobile Security. Any third-party DM framework that can run this file remotely with the correct switches will be able to configure Trend Micro Mobile Security.

Trend Micro provides the Device Management Agent with the latest Trend Micro Mobile Security builds. Setup copies the agent to the following location during installation:

Platform	Location
Windows Mobile	`\Program Files\Trend Micro\Mobile Security\3.0\TmDMAgent.exe`
Symbian	`C:\sys\bin\TmDMAgent.exe`

4.2. Device Management Agent Features

The Device Management Agent has the following features:

- **Scan engine update** (Windows Mobile devices only)—your DM framework can place a new scan engine to a specified folder and call the agent to update Trend Micro Mobile Security.

  Note: New engine releases for the S60 version are packed as PU type SIS files. Typically, your DM framework is able to install these SIS packages directly.

- **Scan pattern update**—your DM framework can place a new scan pattern to a specified folder and call the agent to update Trend Micro Mobile Security.
- **Product settings**—your DM framework can configure the following product settings through the agent:
  - Real-time scan settings
  - Update settings
  - Firewall settings
  - Enable/disable SMS anti-spam
  - Enable/disable WAP Push protection
  - Lock/unlock settings
  - Activation Code
  - URL of the primary and backup update servers

4.3. Using the Device Management Agent

4.3.1. Command Switches and Syntax

To use the agent to update or configure Trend Micro Mobile Security, use your DM framework to run `TmDMAgent.exe` with the correct switches.

Action	Switch/Syntax	Sample
Update scan engine	`/e <path of new engine>`	`…/TmDMAgent.exe /e \temp\vsapice.dll` **Note:** On S60 devices, your DM framework is typically able to install scan engine updates (SIS package) directly.
Update scan pattern	`/p <path of new pattern>`	**Windows Mobile:** `\Program Files\Trend Micro\Mobile Security\3.0\TmDMAgent.exe /p \temp\msvpnwce.108` **S60:** `C:\sys\bin\TmDMAgent.exe /p c:\data\msvpnwce.108`
Configure product	`/o <option>=<option value> <option>=<option value> …` **Note:** See Configuration Options for the list of supported options.	`…/TmDMAgent.exe /o SMSSpamOption=2 LockAllOption=1`

Note: Enclose multi-word values in quotation marks; for example, `/p "\temporary files\ msvpnwce.108"`.

4.3.2. Sending Commands

A device can run only one instance of the Device Management Agent. New instances will automatically exit if the agent is already running.

Typically, your DM framework can queue commands to ensure that only one instance of the agent is running. To help ensure that your commands run successfully, practice the following:

- Whenever possible, submit one command with multiple options instead of separate commands.
- Allow reasonable time between commands to the same device. Submit configuration commands at least five seconds apart and update commands at least one minute apart.

4.3.3. Configuration Options

The Device Management Agent supports the following options for the configuration switch `/o`:

Option	Value	Description
RealTimeScan	0—disable 1—enable	Enable or disable real-time scanner
CompressedFileScanLayer	1, 2, 3	Set number of compression layers to scan
EnableAutoUpdate	0—disable 1—enable	Enable or disable automatic updates
SMSSpamOption	0—disable SMS anti-spam 1—enable blocked list 2—enable approved list	Configure the anti-spam setting
PromptWhenConnectByWireless	0—disable 1—enable	Enable or disable the wireless connection alert
LockAllOption	0—unlock 1—lock all	Prevent or allow users to modify settings through the product interface **Note:** This command option does not cover SMS anti-spam and WAP Push protection settings.
MaxUpdateFrequency	1, 7, 14, 30	Set number of days between forced updates
MinUpdateFrequency	1, 2, 4, 8	Set number of hours between automatic updates, which will run right after the device is connected to the Internet
BlockSMSwoIDOption	0—disable 1—enable	Enable or disable the blocking of SMS messages from unidentified senders
FileScanType	0x7FFFFFFF—all file types 0x3—only executable files 0x7—executable and CAB/ZIP files	Specify the types of files that will be scanned **Note:** This option is not supported in the S60 version.
InstantCardScanOption	0—disable 1—enable	Enable or disable automatic memory card scan
Firewall	0—disable 1—enable	Enable or disable the firewall
IDS	0—disable 1—enable	Enable or disable intrusion detection
SecurityLevel	1—high 2—medium 3—low	Set the firewall security level
ActiveCode	Valid Activation Code	Specify the Activation Code

Option	Value	Description

PrimaryUpdateServer	Valid ActiveUpdate™ URL	Specify the primary update server; you can use the TMCM™ ActiveUpdate server, which by default is:
		`http://<TMCM Web server address>:<port>/TVCSDownload/ActiveUpdate`
		
		Note: To restore to the default settings, deploy a command using the default ActiveUpdate server below as the option:
		`http://mobilesecurity.activeupdate.trendmicro.com/activeupdate`

BackupUpdateServer	Valid ActiveUpdate URL	Specify the backup update server; Trend Micro Mobile Security will use this server if it is unable to access the primary update server.

4.4. Configuration Scenarios

Refer to the scenarios below for examples on how to run common configuration tasks.

Scenario 1

Tasks:

- Activate Trend Micro Mobile Security
- Enable real-time scan
- Enable firewall

Command:

```
TmDMAgent.exe /o ActiveCode=# RealTimeScan=1 Firewall=1
```

Note: # is the Activation Code provided by Trend Micro.

Scenario 2

Tasks:

- Update the Activation Code (extend the current Trend Micro Mobile Security license)

Command:

```
TmDMAgent.exe /o ActiveCode=#
```

Note: # is the updated Activation Code provided by Trend Micro.

Scenario 3

Tasks:

- Enable SMS anti-spam and allow only messages from approved senders
- Prevent users from modifying Trend Micro Mobile Security settings
- Set the product to check all types of files during scans

Command:

```
TmDMAgent.exe /o SMSSpamOption=2 LockAllOption=1 FileScanType= 0x7FFFFFFF
```

Scenario 4

Tasks:

- Enable real-time scan
- Set the product to force updates every seven days
- Set number of maximum compression layers to scan to 2; Trend Micro Mobile Security supports up to three layers of compression for ZIP and CAB files. Multiple compression layers occur when a compressed file is compressed further; for example, when a ZIP file contains another ZIP file.

Command:

```
TmDMAgent.exe /o RealTimeScan=1 MaxUpdateFrequency=7 CompressdFileScanLayer=2
```

Scenario 5

Tasks:

- Set product to block SMS messages from unidentified senders
- Set product to automatically scan memory cards when they are inserted

Command:

```
TmDMAgent.exe /o BlockSMSwoIDOption=1 InstantCardScanOption=1
```

Scenario 6

Tasks:

- Enable firewall
- Enable intrusion detection
- Prevent users from modifying Trend Micro Mobile Security settings

Command:

```
TmDMAgent.exe /o Firewall=1 IDS=1 LockAllOption=1
```

Scenario 7

Tasks:

- Change primary update URL to the default TMCM URL
- Set the product to force updates every seven days
- Enable real-time scan

Command:

```
TmDMAgent.exe /o PrimaryUpdateServer=http://<TMCM Web server address>:<port>
/TVCSDownload/ActiveUpdate RealTimeScan=1 MaxUpdateFrequency=7
```

5. About Trend Micro

Trend Micro Incorporated is a leader in network antivirus and Internet content security software and services. The Tokyo-based Corporation has business units worldwide. Trend Micro products are sold through corporate and value-added resellers, as well as managed service providers. For additional information and evaluation copies of all Trend Micro products, visit http://www.trendmicro.com.