TREND MICRO

TREND MICRO™ Mobile Security 5

Comprehensive security for enterprise handhelds

Deployment Guide

Endpoint Security

Release Date: February 2010

Document Part No.: TSEM53705/80620

The user documentation for Trend Micro™ Mobile Security is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

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

Contents

Chapter 1: Preface

Chapter 1: Server Component Installation

Chapter 2: Mobile Device Agent Component Installation

Preface

Welcome to the Trend Micro™ Mobile Security for Enterprise v5.5 Deployment Guide. This guide assists administrators in deploying and managing Trend Micro Mobile Security for Enterprise v5.5. This guide describes various Mobile Security components and the different mobile device agent deployment methods.

For updated information about Mobile Security, including mobile device support and the latest builds, visit http://us.trendmicro.com/us/products/enterprise/mobile-security/index.html.

Note: This Deployment Guide applies only to Mobile Security version 5.5. It does not apply to other versions of Mobile Security. Trend Micro support is limited to the use of Mobile Security. To obtain support for third-party applications mentioned in this guide, contact their corresponding vendors.

This preface discusses the following topics:

Audience

The Mobile Security documentation is intended for both administrators—who are responsible for administering and managing Mobile Security devices in enterprise environments—and device users.

Administrators should have an intermediate to advanced knowledge of Windows system administration and mobile device policies, including:

- Installing and configuring Windows servers
- Installing software on Windows servers
- Configuring and managing mobile devices (such as smartphones and Pocket PC/Pocket PC Phone)
- Network concepts (such as IP address, netmask, topology, and LAN settings)
- Various network topologies
- Network devices and their administration
- Network configurations (such as the use of VLAN, HTTP, and HTTPS)

Mobile Security Documentation

The Mobile Security documentation consists of the following:

- **Administrator's Guide**—this guide provides detailed Mobile Security configuration policies and technologies.
- **Deployment Guide**—this guide helps you get "up and running" by introducing Mobile Security, and assisting with network planning and installation.
- **User's Guide**—this guide introduces users to basic Mobile Security concepts and provides Mobile Security configuration instructions on their mobile devices.
- **Online help**—the purpose of online help is to provide "how to's" for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values.
- **Readme**—the Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a description of new features, installation tips, known issues, and release history.

- **Knowledge Base**— the Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, open:

  http://esupport.trendmicro.com/

Tip: Trend Micro recommends checking the corresponding link from the Update Center (http://www.trendmicro.com/download) for updates to the product documentation.

Document Conventions

To help you locate and interpret information easily, the documentation uses the following conventions.

CONVENTION	DESCRIPTION
ALL CAPITALS	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, options, and tasks
Italics	References to other documentation
Monospace	Example, sample command line, program code, Web URL, file name, and program output
Link	Cross-references or hyperlinks.

CONVENTION	DESCRIPTION
Note:	Configuration notes
Tip:	Recommendations
WARNING!	Reminders on actions or configurations that should be avoided

Chapter 1

Server Component Installation

This chapter assists administrators in planning and installing the server components for Trend Micro Mobile Security 5.5.

This chapter contains the following sections:

Planning Server Installation

Before you install Mobile Security for Enterprise v5.5, read this section for system requirements.

Network Planning

Mobile Security for Enterprise v5.5 consists of four components: Mobile Security Management Module (MSMM), Mobile Security Communication

Manager (MSCM) server, SMS senders, and Mobile Device Agent (MDA). *Figure 1-1* shows where each Mobile Security component resides in a typical network.

Depending on your company needs, you can implement Mobile Security with different client-server communication methods. You can also choose to set up one or any combination of client-server communication methods in your network.

Tip: You can install a proxy server or firewall between the MSCM server and the Mobile Device Agents outside the intranet. To configure proxy settings, log on to the Mobile Security Management server and click **Plug-in Manager**. Then click **Manage Program for Mobile Security** and click **Administration > Connection Settings**.

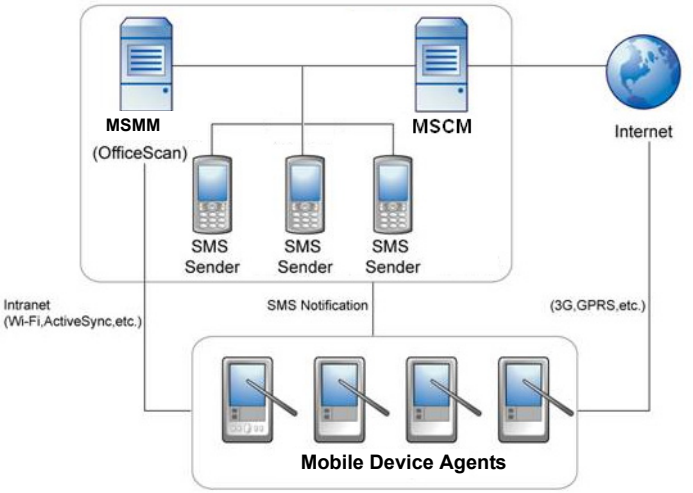

FIGURE 1-1. Mobile Security components

System Requirements

Review the following requirements before installing each Mobile Security component in your network. For information on Mobile Security components, refer to the Mobile Security 5.5 Administrator's Guide.

TABLE 1-1. System Requirements

COMPONENT	REQUIREMENTS
Mobile Security Management Module (MSMM)	• OfficeScan server 8.0 • Plug-in Manager 1.0 (build 3093) or • Officescan server 10.0 SP1 • Officescan server 10.0 • OfficeScan server 8.0 SP1 • Plug-in Manager 1.0 (build 3163) **Note:** Refer to the OfficeScan Client/Server Edition 8.0/10.0 server documentation for minimum system requirements.

TABLE 1-1. System Requirements

COMPONENT	REQUIREMENTS
Mobile Security Communication Manager (MSCM) server	**Platform** • Microsoft™ Windows™ 2000 Advanced Server SP4 • Microsoft Windows 2003 Standard Server SP2 (32-bit) • Microsoft Windows 2003 R2 Enterprise Server (64-bit) • Microsoft Windows 2008 Standard Server SP2 (32-bit) • Microsoft Windows 2008 R2 Enterprise Server (64-bit) **Hardware** • 800MHz Intel™ Pentium™ processor or equivalent • At least 512MB of RAM • At least 40MB of available disk space • USB support • A monitor that supports 800 x 600 resolution at 256 colors or higher
SMS Sender	• Windows Mobile 5 Pocket PC Phone • Windows Mobile 5 Smartphone • Windows Mobile 6 Standard • Windows Mobile 6 Professional

TABLE 1-1. System Requirements

COMPONENT	REQUIREMENTS
Web server	• Microsoft Internet Information Server (IIS) 5.0/6.0/7.0/7.5 • Apache 2.x or above **Note:** When using IIS 7.0 or above for MSMM or MSCM, verify that "CGI", "ISAPI Extensions" in Application Development, and "II6 management compatibility" are installed and enabled. When using IIS with a 64-bit OS, set "Enable 32-Bit Applications".
Web browser	Internet Explorer 5.5/6.0/7.0/8.0

Installing Server Components

Before you proceed to install Mobile Security server components, make sure the Mobile Security components meet the specified system requirements. You may also need to evaluate your network topology and needs to determine the Mobile Security server components you want to install.

This section shows you how to install the following Mobile Security server components:

- Mobile Security Management module—plug-in program on the Mobile Security Management server
- MSCM server—the server that handles communication between the MSMM and a Mobile Device Agents (MDA) or SMS senders
- SMS Sender—a mobile device that connects to the MSMM or MSCM server to send SMS messages

Installing the Mobile Security Management Module

Before you can install Mobile Security Management Module (MSMM), make sure you have already installed the OfficeScan server version 8.0/10.0 (including SP1) and Plug-in Manager 1.0.

To install MSMM:

1. Log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.
3. Click **Download** to get the Mobile Security Plug-in package. The package also includes installation files for the SMS Sender, MSCM server, and Mobile Device Agent.
4. Click **OK** to start the file download process. Wait until the file download is completed.
5. Click **Install Now**.
6. Click **Accept** to agree with the end-user license and start the installation process.

Accessing the MSMM Web Console

You can access the management console for MSMM through the OfficeScan Web console.

To access the MSMM Web console:

1. Log on to the OfficeScan Web console and click **Plug-in Manager**.
2. Click **Manage Program** for Mobile Security.

Installing the MSCM Server

Installation of the MSCM server is optional. You only need to install the MSCM server if you want to:

- reduce the load on the Mobile Security Management Module for device component updates and monitoring
- allow Mobile Device Agents to update components and synchronize configuration over the Internet and provide an additional layer of security for the Mobile Security Management Module.

Note: Trend Micro recommends installing the MSCM server on another computer.
Before you proceed with the MSCM installation, make sure you have installed IIS or Apache Web server on the computer.
With IIS Web server, the MSCM server supports both HTTP and HTTPS (default) connection types.
With the Apache Web server, the MSCM server supports HTTP connection type by default. To allow HTTPS connection, manually configure your Apache Web server settings.

To install the MSCM server:

1. On the Mobile Security Management server, copy the setup file from the folder `\OfficeScan\Addon\Mobile Security\AgentPackage\MSCMServer` to the computer on which you want to install the MSCM server.
2. Double-click the setup file to start the installation process.
3. Follow the on-screen instructions.
4. Select an IP address and type a service port number for the MSCM server. The IP address and port number are used for the MSCM server to communicate with the MSMM (Trend Micro recommends selecting "ALL" for IP address. This will allow this value to auto-update if there is an IP change).

Installing SMS Sender

You only need to install an SMS sender if you want to use the SMS messaging feature for notifications.

Install SMS senders to send messages that notify Mobile Device Agents to:

- download and install Mobile Device Agent
- register to the Mobile Security Management Module
- update components from the Mobile Security Management Module
- synchronize configuration with the Mobile Security Management Module
- remote wipe the mobile device
- remote lock the mobile device if encryption is enabled

You can install and connect up to 64 SMS senders to the MSCM server over Wi-Fi connections.

WARNING! **If you connect an SMS sender to a host computer using ActiveSync and a firewall is installed on the MSCM server, you must configure the firewall rule to allow traffic on port 5721. Otherwise, the SMS sender cannot receive instructions from the MSCM server to send messages to mobile devices.**

To install an SMS sender:

1. On the Mobile Security Management server, copy the setup file from the folder `\OfficeScan\Addon\Mobile Security\AgentPackage\SmsSender` to a memory card for the supported device platform.
2. Insert the memory card to the device. Open the setup file to install the SMS Sender program. You can install the SMS Sender on the memory card or on a phone.
3. From the **Start** menu, open **SMS Sender Setup** in the **Programs** folder to configure MSMM/MSCM server and phone settings. In the **SMS Sender Config** screen, do the following:
   - Type the DNS name or IP address of the server
   - Type the HTTP port number of the server
   - Type the phone number to send SMS notifications
   - Select the encoding method for SMS notifications

Note: By default, SMS senders use unicode to encode SMS messages. If errors occur when sending or receiving SMS messages in unicode, change the encoding method to "7-bit GSM".

Installing Server Components with a Local Update Source

If the Mobile Security Management server is unable to connect to the Internet, you need to install the Mobile Security server components on the Mobile Security Management server (localhost) and specify local update sources for Mobile Security.

Note: Before you continue, obtain the installation package from your Trend Micro sales representative. The installation package will contain the setup files for Mobile Security agent and server components.

To install Mobile Security for Enterprise v5.5 with a local update source:

1. On the Mobile Security Management server, create a virtual directory "TmmsAu".
   - If you are using IIS Web server, open the Internet Information Services (IIS) Manager screen and right-click **Default Web Site**. Then click **New > Virtual Directory**.
   - If you are using Apache Web server, specify the new virtual directory in the `httpd.conf` file and restart the Apache service. The following shows an example of the virtual directory section for "TmmsAu" in the `httpd.conf` file.

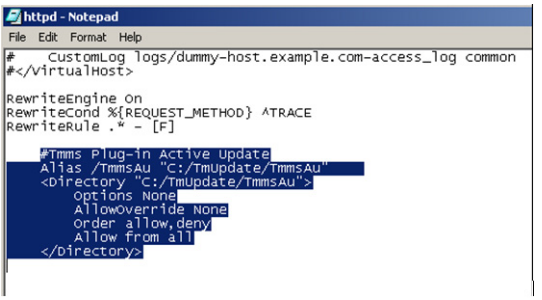

FIGURE 1-2. Apache httpd.conf example for a new virtual directory

2. Extract the installation package from Trend Micro.
3. Copy the folders " TmmsServerAu" and "TmmsClientAu" to the virtual directory. If prompted, accept to overwrite any existing folders in the directory.

To specify a local update source for OfficeScan:

1. Log on to the OfficeScan Web console and click **Updates > Update Source**. The Server Update Source screen displays.
2. Select **Other update source** and type "http://localhost/TmmsAu/TmmsServerAu" in the field provided. Click **Save**.
3. Restart the OfficeScan Plug-in Manager service to make the changes take effect.
4. Log on to the OfficeScan Web console again and click **Plug-in Manager**.
5. Follow the on-screen instruction to download and install Mobile Security on the Mobile Security Management server.
6. After the installation is completed, click **Manage Program** to access the configuration screens for Mobile Security.
7. Type the Activate Code to register the product. Refer to *Registering the Product* on page 1-12 for more information. After product registration is completed successfully, the **Summary** screen for Mobile Security displays.

To specify a local update source for Mobile Security:

1. Log on to the OfficeScan Web console and click **Plug-in Manager**. Then, click **Manage Program** for Mobile Security.
2. Click **Updates > Server Update** and click the **Source** tab to configure the update source for Mobile Security components.

3. Select **Other update source** and type `http://localhost/TmmsAu/TmmsClientAu` in the field provided. Click **Save**.
4. To verify the policies, perform a manual update (click **Updates > Server Update > Manual**).

Initial Server Setup

This section walks you through the initial setup of Mobile Security Management Module after the server installation.

Initial server setup steps include:

- *Registering the Product* on page 1-12
- *Connection Settings* on page 1-14
- *Configuring SMS Sender List* on page 1-16

Note: You must complete the initial server setup for the Mobile Security Management Module before you continue to install Mobile Device Agent on mobile devices. You cannot access the management console for Mobile Security through Trend Micro Control Manager™.

Registering the Product

Trend Micro provides all registered users with technical support, malware pattern downloads, and program updates for a specified period after which you must purchase renewal maintenance to continue receiving these services. Register Mobile Security Management Module to ensure that you are eligible to receive the latest security updates and other product and maintenance services.

The type of Mobile Security Activation Code (also known as a serial number) you purchase determines whether the encryption module is included with Mobile Security Management Module. Please consult your local Trend Micro sales representative for more information.

You only need to register Mobile Security Management Module on the Mobile Security Management server using the Activation Code. Mobile Device Agents automatically obtain license information from the Mobile Security Management Module after the mobile devices are connected and registered to the server.

If the encryption module is activated on the Mobile Security Management Module and the encryption policy is configured, Mobile Device Agents will install the encryption module on the supported mobile devices after product registration is successful.

Activation Code Format

An activate code displays in the following format:

`xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx`

To register Mobile Security Management Module:

1. Log on to the OfficeScan Web console and click **Plug-in Manager**.
2. Click the **Manage Program** button for Mobile Security. If this is the first time you access the management console, the Product License screen displays; otherwise, click **Administration** > **Product License** and click **New Activation Code**.
3. Type the Activation Code in the fields provided and click **Save**.

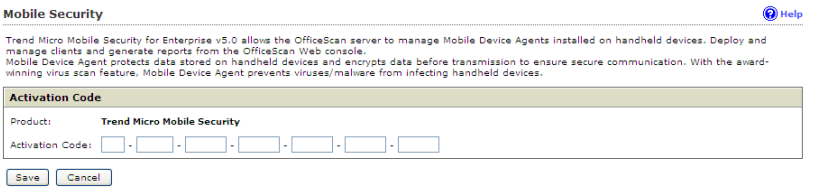

FIGURE 1-3. Registering Mobile Security after installation

4. Verify that product registration is successful. Click **Summary** to display the Summary screen. You should see the message "Trend Micro Mobile Security is activated" if product registration is successful.

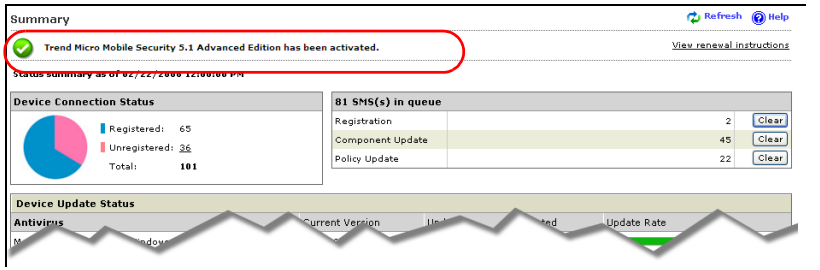

FIGURE 1-4. Successful product registration

Connection Settings

Use the **Connection Settings** screen to configure the following connection settings for Mobile Security:

- 3G/GPRS—allows Mobile Device Agents on mobile devices to communicate with the Mobile Security Management Module over the Internet. Mobile devices can also connect directly or through a proxy to the Mobile Security Management Module for component/policy updates and log reporting.

  Note: For 3G/GPRS communication, if the proxy or Mobile Security Management server is behind a NAT device, you must configure port mapping settings to map the private IP address to the DNS name or public IP address. If the proxy or Mobile Security Management server is behind a firewall, make sure you have configured firewall policies to allow traffic from mobile devices.

- MSCM server connection—allows the Mobile Security Management Module to connect to the MSCM server to handle requests from Mobile Device Agent and SMS senders.

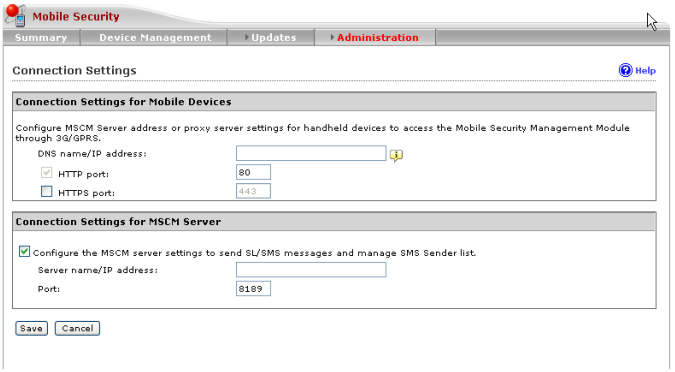

FIGURE 1-5. Connection Settings

To configure 3G/GPRS connection settings:

1. Log on to the OfficeScan Web console and click **Plug-in Manager**.
2. Click the **Manage Program** button for Mobile Security.
3. Click **Administration** > **Connection Settings**.
4. In the **DNS name / IP address** field, type the public DNS name or IP address of the proxy or Mobile Security Management server on which you installed Mobile Security Communication Manager.
5. Specify the protocol and port number for 3G/GPRS communication.

   By default, the Mobile Security Communication Manager uses **HTTP** protocol on port 80 for 3G/GPRS connections. If you want to use a different HTTP port, type the port number.

   For secure connection, select **HTTPS** and specify the service port number in the field provided (for example, 443).
6. Click **Save**.

WARNING! HTTPS connection setting does not apply to Symbian devices. Symbian devices will only use HTTP connection to communicate with Mobile Security Management Module or Mobile Security Communication Manager.

To configure MSCM server connection settings:

1. Log on to the OfficeScan Web console and click **Plug-in Manager**.
2. Click the **Manage Program** button for Mobile Security.
3. Click **Administration** > **Connection Settings**.
4. Select the check box **Configure the MSCM server settings** to allow the Mobile Security Management Module to send instructions to the MSCM server.
5. In the **Server Name/IP Address** field, type the name or IP address of the MSCM server.
6. In the **Port** field, type the service port the MSCM server. The default port number is 8189.
7. Click **Save**.

Note: If a firewall is installed between the MSCM server and the Mobile Security Management server, a host computer for an SMS sender, or a proxy server, you need to configure firewall policies to allow traffic to the specified port on the MSCM server.

To verify the connection to the MSCM server:

1. After configuring the MSCM server, log on to the Mobile Security Management server Web console and click **Plug-in Manager** in the main menu.
2. Click **Manage Program** for Mobile Security. The Summary screen displays. If there is no error message "MSCM Server unreachable", this means the Mobile Security Management Module is able to connect to the MSCM server successfully.

Configuring SMS Sender List

You must type the SMS sender information in the Web console to allow communication between the Mobile Security Management Module and the SMS sender.

To configure an SMS sender phone number:

1. Log on to the Mobile Security Management Web console and click **Plug-in Manager**.
2. Click **Manage Program** for Mobile Security.
3. Click **Administration > SMS Sender Settings** > **SMS Sender List**

4. In the SMS Sender List tab, click **Add**.

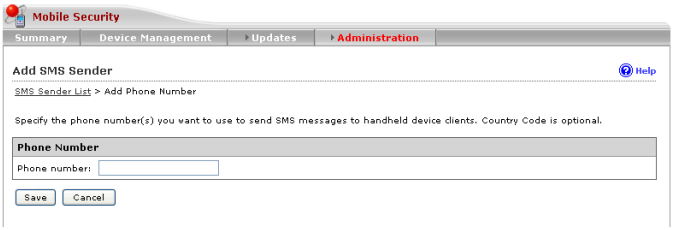

FIGURE 1-6. Add SMS Sender screen

5. In the **Add SMS Sender** screen, type the phone number of an SMS sender and click **Save**.

WARNING! **Ensure the phone number used here is the same as the one configured on the SMS sender device. If not, the SMS sender will not be able to connect to the MSMM/MSCM server.**

6. The **SMS Sender List** screen displays. Check that the **Status** field displays "Connected" for the number you have configured. If the **Status** field displays "Disconnected", make sure the SMS sender can connect to the MSMM/MSCM server.

Note: For information on upgrading TMMS from 5.0 or 5.1 server components, see the *Administrator's Guide*.

Chapter 2

Mobile Device Agent Component Installation

This chapter discusses the different mobile device agent deployment methods. Mobile device requirements and models that Mobile Device Agent supports are also included.

This chapter contains the following sections:

Planning Mobile Device Agent Installation

Note: Make sure the mobile devices can connect to the Mobile Security Management Module through Wi-Fi, 3G/GPRS, or using the Internet connection on a host computer.

Supported Mobile Devices and Platforms

Before installing and using the Mobile Security mobile device agent program (known as the Mobile Device Agent) on mobile devices, ensure that your mobile devices meet the requirements.

Device Storage and Memory

TABLE 2-1. System 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
Symbian OS 9.x S60 3rd/5th Edition	2	2

Mobile Device Agent Installation Methods

You can install Mobile Device Agent on mobile devices using one of the following methods:

- Silent installation through SMS messages—sends SMS messages with Mobile Device Agent installation URL to mobile devices. Depending on whether the service provider allows SL messaging, Mobile Device Agent installation and registration are automatic on mobile devices or users need to click the URL in the SMS message to start the process. You need to install the SMS senders.
- Memory card—download the setup file from the Mobile Security Management Module and copy the extracted files to a memory card. Once you insert the memory card into a mobile device, Mobile Device Agent installation and registration is automatic.

Note: Memory card installation method is not available if you want to re-install or upgrade Mobile Device Agent for Mobile Security 5.5 on Symbian devices. In this case, you should use the manual installation method.

- Device Management (DM) framework—allows you to install Mobile Device Agent using third-party software such as Nokia™ Intellisync™, Sybase™ iAnywhere Afaria™, and Odyssey Software™ Athena™. You will need to extract the setup files for the supported mobile devices and configure the DM framework to send (or push) the setup files. Refer to the documentation that comes with your DM framework for instructions.
- Manual install—requires you to transfer setup files to each mobile device and run the setup program. After the installation is completed, you then need to register Mobile Device Agents to the Mobile Security Management Module. For detailed instructions on manual installation and registration, refer to *Launching the Setup File Manually* on page 2-9 or the User's Guide for your mobile device platform.

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 previous versions before installing Mobile Security 5.5.

Note: If your Windows Mobile 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.

Installing Mobile Device Agent

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

- disable the password security or memory card encryption feature that comes with Windows Mobile on your mobile device
- remove any third-party password security program. You may be prompted to remove the program during the installation process.

Note: The encryption module will not work if the built-in password security or the memory card encryption feature is enabled.

Silent Installation Using SMS Notifications

Installing the Mobile Device Agent through SMS notifications involves the following steps:

- *Configuring SMS Sender List* on page 1-16
- *Configuring Installation Message* on page 2-4
- *Configuring the Mobile Device List* on page 2-6

Configuring Installation Message

To initiate silent Mobile Device Agent installation, SMS senders send a WAP Push (Service Load) message and an SMS message to notify mobile devices to download and install Mobile Device Agent.

If a mobile device is unable to process the Service Load (SL) message, users can still open the SMS message to download the Mobile Device Agent setup package by clicking the URL included in the message.

You can use the **Installation Message** screen to type the message you want to display in the SMS message.

To configure installation message:

1. Log on to the OfficeScan Web console and click **Plug-in Manager**.
2. Click **Manage Program** for Mobile Security.
3. Click **Administration** > **SMS Settings**.
4. Click the **Installation Message** tab. The Installation Message screen displays.

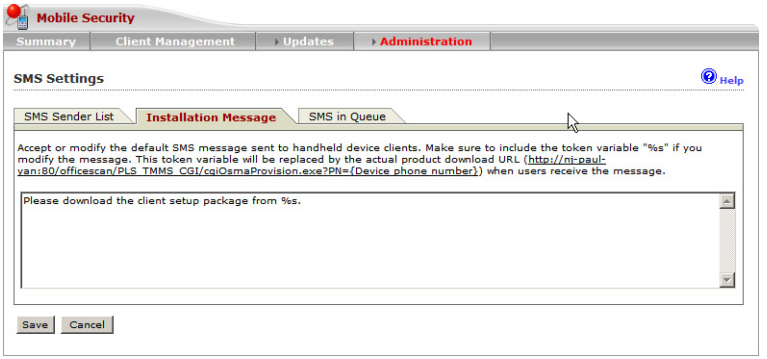

FIGURE 2-1. Setting the installation message

5. Type the message in the text box.

Note: The installation message must include the characters "%s" which will automatically be replaced with the URL that allow users to download the Mobile Device Agent setup file.

---

6. Click **Save**.

Configuring the Mobile Device List

Configure the mobile device list on the Mobile Security Management Module if you want to send SMS messages to specified mobile devices. You must first configure the mobile device agent list before SMS Senders can notify mobile devices to install and register Mobile Device Agents.

If you install Mobile Device Agent manually, through a device management (DM) framework, or using a memory card, the Mobile Security Management Module will automatically add Mobile Device Agent information to the list after the device is registered to the Mobile Security Management Module.

To add a device:

1. Log on to the OfficeScan Web console and click **Plug-in Manager**.
2. Click the **Manage Program** button for Mobile Security.
3. Click **Device Management**. The Device Management screen displays.
4. Click the **Manage Device Tree** tab and select **Add Device**.

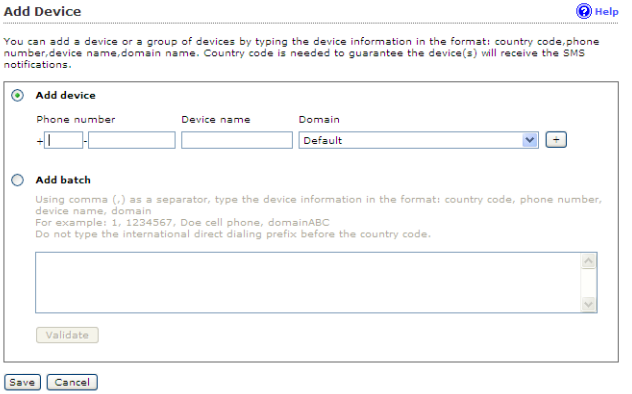

FIGURE 2-2. Adding a device

5. Select **Add device** and configure the following fields:
   - **Phone number**—type the phone number of a mobile device

Note: To ensure that the mobile device can received notification messages successfully from an SMS sender, you must type the country code (1-5 digits long). You do not have to type the international direct dialing prefix.

- **Device name**—type the name of the mobile device to identify the device in the device tree
- **Domain**—select the name of the domain to which the mobile device belongs from the drop-down list. If you do not select a domain from the list, the mobile device agent is added to the "default" domain. You can always change the domain to which the mobile device agent belongs.

Tip: To add more devices, click the + button.
Alternatively, you can select **Add batch** and type the device information in the text box. Click **Validate** to verify that the device information conforms to the specified format.

6. Click **Save**.
7. Check that the new device information is displayed in the device tree. After you have added information for the mobile devices on the Mobile Security Management Module, refer to the next section to install Mobile Device Agent on these mobile devices.

Checking Mobile Device Agent Status

After you have saved the mobile device information on the Mobile Security Management Module, SMS senders automatically send SMS messages to notify the mobile devices to start Mobile Device Agent download and installation. After the installation is completed successfully, Mobile Device Agent automatically registers to the Mobile Security Management Module. The file download, product installation, and registration may take several minutes.

You can check the mobile device agent registration status in the Summary screen for Mobile Security in the Mobile Security Management server.

Installing Using Memory Card

You can use a memory card to manually install Mobile Device Agent on mobile devices. You need to download the setup file from the Mobile Security Management Module and extract the files to a memory card.

WARNING! ***Memory card installation method is not available if you want to re-install or upgrade Mobile Device Agent on a Symbian device. In this case, you should use the manual installation method.***

To obtain setup files from the Mobile Security Management Module:

1. Log on to the OfficeScan Web console and click **Plug-in Manager**.
2. In the Plug-in Manager screen, click **Manage Program** for Mobile Security.
3. Click **Administration** > **Device Setup File**.
4. Click **Download** to download the ZIP file to your computer.
5. Extract the ZIP file.
6. Copy the extracted files to the root folder in a memory card.

Note: If you are using Apache Web server and the setup package is opened as a text file, you need to modify Apache Web server settings. You can replace `"DefaultType text/plain"` with `"application/octet-stream"` in the file "conf/http.conf" or add `"sis cab zip"` after the line `"application/octet-stream"` in the file `"conf/mime.types"`.

If the extracted files are not located in the root folder in the memory card, automatic installation will not work when you insert the card in to a mobile device.

To install Mobile Device Agent on a mobile device:

1. Insert the memory card into a mobile device. Setup automatically installs Mobile Device Agent.
2. After the installation is complete, restart your mobile device when prompted.
3. Your mobile device automatically registers to the Mobile Security Management server. Select an AP your mobile device is to use to connect to the Mobile Security Management server. Mobile Security is added to the **Start** menu.

The registration process may take several minutes. To verify that mobile device agent registration is successful, check the Mobile Device Agent status in the device tree on the Mobile Security Management Module.

Launching the Setup File Manually

You can execute the setup file on a mobile device to manually install Mobile Device Agent. To transfer the setup file to the mobile device, you need to use ActiveSync or PC Suite to connect the mobile device to a host computer. After the installation is completed successfully, you must manually register Mobile Device Agent to the Mobile Security Management Module.

Note: On Symbian devices:
- you can execute the setup file directly on a host computer with PC Suite

To obtain setup files from the Mobile Security Management Module:

1. Log on to the OfficeScan Web console and click **Plug-in Manager**.
2. In the Plug-in Manager screen, click **Manage Program** for Mobile Security.
3. Click **Administration** > **Device Setup File**.
4. Click **Download** to download the ZIP file to your computer.
5. Extract the ZIP file and copy the extracted files to a host computer.
6. The administrator will have to determine the best way to send this file to the user. This could, for example, be done through an email or on a helpdesk site in an Intranet.

   The user can also be provided the installation file:

   Transfer the appropriate setup file to the mobile device or execute the setup file on a host computer with PC Suite (for Symbian devices only).

   - Windows Mobile 5 for Smartphone or Windows Mobile 6 Standard: `MobileSecurity_SP.cab`
   - Windows Mobile 5 for Pocket PC/Pocket PC Phone or Windows Mobile 6 Professional/Classic: `MobileSecurity_PPC.cab`
   - Symbian OS 9.x S60 3rd/5th Edition on Nokia mobile device: `MobileSecurity_S60.sis`

Alternatively, the user can be instructed to download and install the mobile device agent by visiting the URL.

For users that are in the internal network with access to the Server:

```
http(s)://<Office scan Server:Port>/officescan/
PLS_TMMS_CGI/cgiOsmaProvision.dll
```

For users that are roaming and can not access the internal network:

```
http://<Public Address:Port>/officescan/
PLS_TMMS_CGI/cgiOsmaProvision.dll
```

Note: If you are using Apache Web server and the setup package is opened as a text file, you need to modify Apache Web server settings. You can replace `"DefaultType text/plain" with "application/octet-stream"` in the file "conf/http.conf" or add `"sis cab zip"` after the line `"application/octet-stream"` in the file `"conf/mime.types."`

You can also obtain the Mobile Device Agent setup files directly from the server at the following location:

```
http(s)://<Office scan Server:
Port>/officescan/PLS_TMMS_ActiveUpdate/<Setup Package
Name>

<Setup Package Name> the setup package names on the
server are as follows:
PPC: MobileSecurity_PPC.cab
SP: MobileSecurity_SP.cab
Symbian S60 3rd/5th on Nokia mobile device:
MobileSecurity_S60.sis
```

To manually install Mobile Device Agent on mobile devices:

1. On your device, navigate to the location of the setup file.
2. Open the setup file to start installing the Mobile Device Agent.
3. After the installation completes, copy the file `TmSettings.ini` to the appropriate directory on the handset:

   ```
   \Program Files\Trend Micro\Mobile Security\(for Windows
   Mobile)
   ```

```
C:\system\data\mobilesecurity\ (Symbian OS requires a
3rd-party file explorer to access this directory)
```

4. Restart the device. The device will automatically register to the server.

Manual Registration

You will need to manually register Mobile Device Agent to the Mobile Security Management Module if you install Mobile Device Agent manually or if the automatic registration process fails.

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

1. Open Mobile Device Agent program on the mobile device. On Windows Mobile platforms, if this is the first time you access the display, you may be prompted to type the power-on password.
2. The **Register** screen displays. Type a descriptive name for the device, the DNS name or IP address and HTTP port number of the Mobile Security Management server (where the Mobile Security Management Module is installed). Click **Register**.

   Note: You can only use HTTP port for manual registration. Check the HTTP port on your web server where the Mobile Security management Module is installed.

3. After the registration is completed, view the license information in the About screen (**Menu** > **About**). You can also see the device status on the Mobile Security Management Module. Note that the registration process may take several minutes.

Using Device Management Framework

This section describes how to deploy and manage Mobile Device Agent 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.

To deploy Mobile Device Agent using DM framework:

1. Log on to the OfficeScan Web console and click **Plug-in Manager**.
2. In the Plug-in Manager screen, click **Manage Program** for Mobile Security.

3. Click **Administration** > **Device Setup File**.
4. Click **Download** to download the ZIP file to your computer.
5. Extract the ZIP file.
6. Copy the extracted files and `TmSettings.ini` to the DM framework server. On the DM framework server, save the file `TMsettings.ini` to `\Program Files\Trend Micro\Mobile Security\` (for Windows Mobile) or `C:\data\mobilesecurity\` (for Symbian OS).
7. Send the command to execute the setup file on the devices to install Mobile Device Agent.
8. After the installation is completed, Mobile Device Agent automatically registers to the Mobile Security Management Module.

Using the Encryption Module

The encryption module provides the power-on password and encryption features on your mobile device.

Encryption module can be used on a mobile device if all of the following requirements are met:

- Mobile Device Agent is installed successfully
- Mobile Device Agent has successfully registered to the Mobile Security Management Module
- the encryption license is included in the product license, and encryption is enabled
- the encryption module supports the mobile device platform

Note: Encryption module in Mobile Security 5.5 supports Windows Mobile 5/6 operating system, but does not support Symbian S60 3rd/5th.

- the default system lock or card encryption function are not enabled on the mobile device

To use the encryption module:

1. After installing Mobile Device Agent, register the Mobile Device Agent to the Mobile Security Management Module. To register the Mobile Device Agent, refer to *Manual Registration* on page 2-11.
2. Restart the mobile device to activate the encryption module. When the mobile device finishes restarting and registering to the network, the **Password** screen displays. After registration, you are prompted to provide an initial power-on password to log on the device. By default, the initial password is **123456**.

Note: If the license for encryption expires, encryption is disabled on your device.