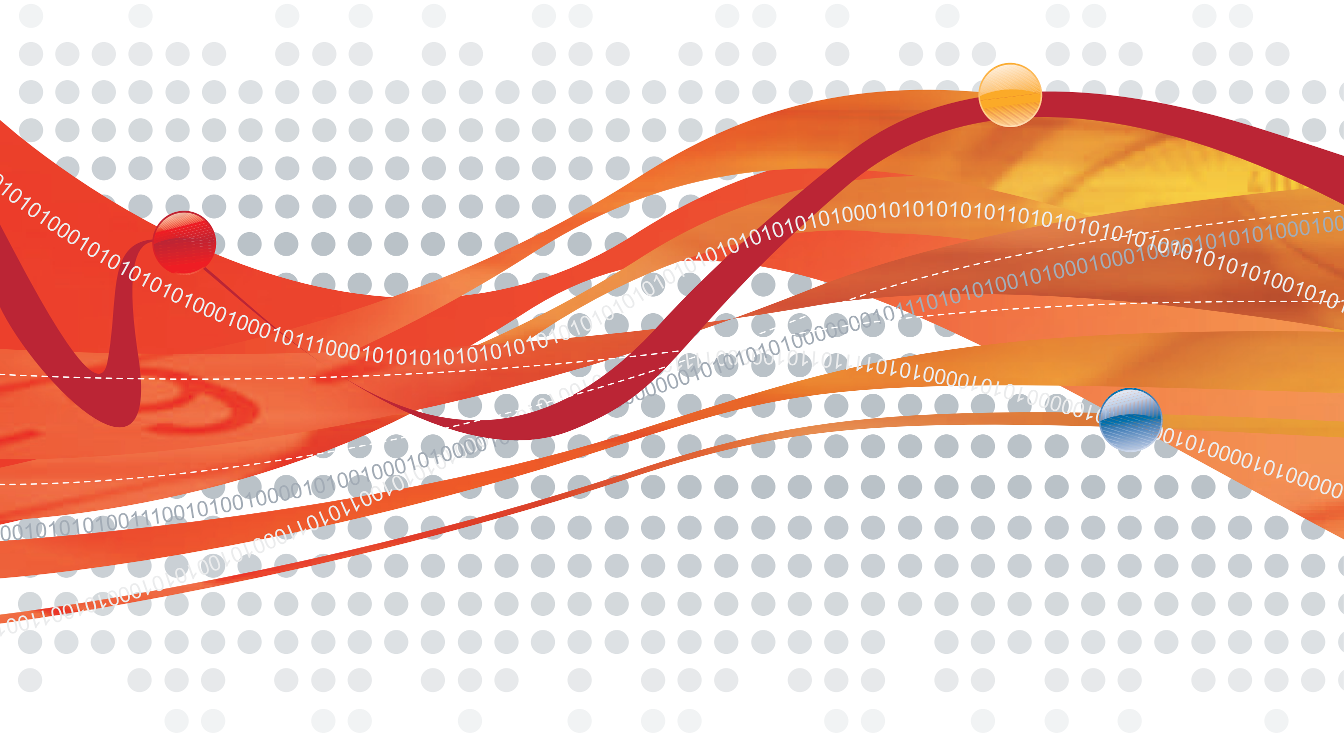
TREND MICRO™

TREND MICRO™ Mobile Security 7

Comprehensive security for enterprise handhelds

Installation and Deployment Guide



Endpoint Security

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

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

Release Date: September 2011

Document Part No.: TSEM74852/110520

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

Preface

Chapter 1: Server Component Installation

Chapter 2: Mobile Device Agent Component Installation

Preface

Preface

Welcome to the Trend Micro™ Mobile Security for Enterprise 7.1 Installation and Deployment Guide. This guide assists administrators in deploying and managing Mobile Security for Enterprise 7.1. 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 Installation and Deployment Guide applies only to Mobile Security version 7.1. 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* on page iv
- *Mobile Security Documentation* on page iv
- *Document Conventions* on page v

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.
- **Installation and 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 for Enterprise 7.1.

This chapter contains the following sections:

Planning Server Installation

Before you install Mobile Security for Enterprise 7.1, read this section for system requirements.

Network Planning

Mobile Security for Enterprise 7.1 consists of the following four components:

- Master Server
- Policy server
- SMS Senders (optional)
- Mobile Device Agent (MDA)

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.

Trend Micro Mobile Security supports two different models of deployment:

- Basic Security Model (Single Server Installation)
- Enhanced Security Model (Dual Server Installation)

Basic Security Model (Single Server Installation)

The Basic Security Model supports the installation of Policy Server and Master Server on the same computer. *Figure 1-1* shows where each Mobile Security component resides in a typical Basic Security Model.

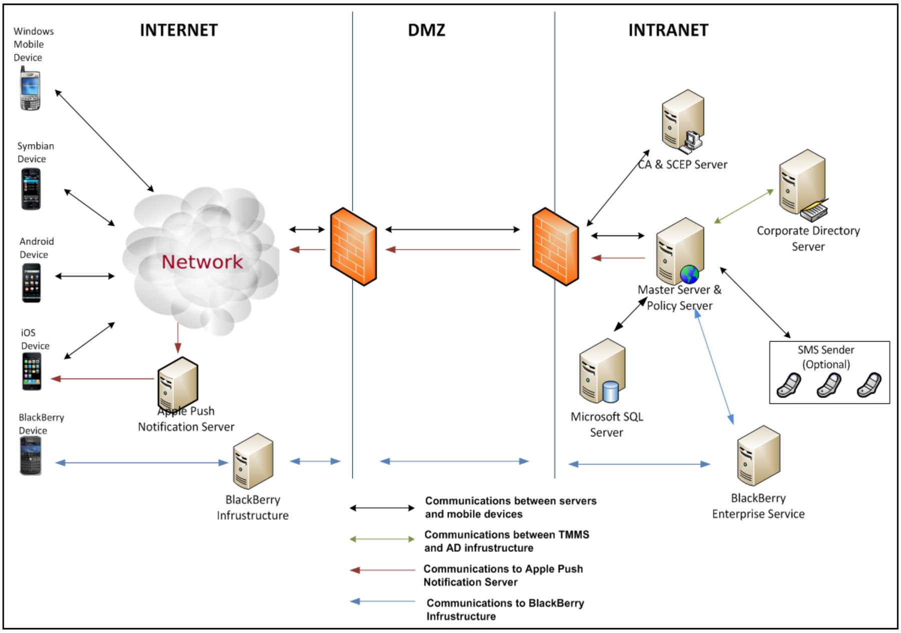

Windows Mobile Device
INTERNET
DMZ
INTRANET
Symbian Device
Android Device
iOS Device
BlackBerry Device
Network
Apple Push Notification Server
BlackBerry Infrustructure
CA & SCEP Server
Corporate Directory Server
Master Server & Policy Server
SMS Sender (Optional)
Microsoft SQL Server
BlackBerry Enterprise Service
Communications between servers and mobile devices
Communications between TMMS and AD infrustructure
Communications to Apple Push Notification Server
Communications to BlackBerry Infrustructure

FIGURE 1-1. Basic Security Model

Enhanced Security Model (Dual Server Installation)

The Enhanced Security Model supports the installation of Policy Server and Master Server on two different server computers. *Figure 1-2* shows where each Mobile Security component resides in a typical Enhanced Security Model.

WARNING! Trend Micro strongly recommends deploying the Enhanced Security Model on two server computers. This model provides maximum security.

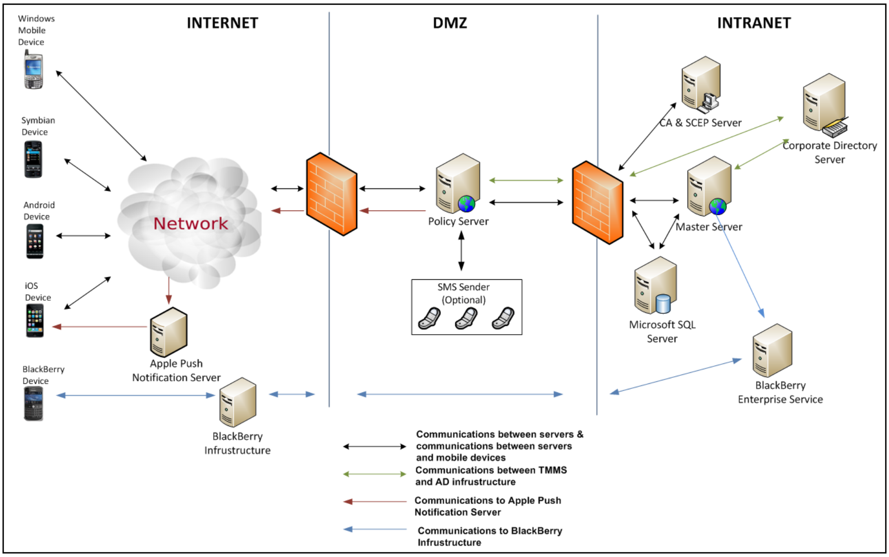

INTERNET
DMZ
INTRANET
Windows Mobile Device
Symbian Device
Android Device
iOS Device
BlackBerry Device
Network
Apple Push Notification Server
BlackBerry Infrustructure
Policy Server
SMS Sender (Optional)
CA & SCEP Server
Corporate Directory Server
Master Server
Microsoft SQL Server
BlackBerry Enterprise Service
Communications between servers & communications between servers and mobile devices
Communications between TMMS and AD infrustructure
Communications to Apple Push Notification Server
Communications to BlackBerry Infrustructure

FIGURE 1-2. Enhanced Security Model

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 for Enterprise 7.1 Administrator's Guide.

TABLE 1-1. System Requirements

COMPONENT	REQUIREMENTS
Master Server	• OfficeScan server 8.0 • Plug-in Manager 1.0 (build 3093) or • OfficeScan server 10.5 SP2 • OfficeScan server 10.5 SP1 • OfficeScan server 10.5 • OfficeScan server 10.0 SP1 • OfficeScan server 10.0 • OfficeScan server 8.0 SP1 • Plug-in Manager 1.0 (build 3163) or • OfficeScan server 10.6 • OfficeScan server 10.5 SP2 • OfficeScan server 10.5 SP1 • OfficeScan server 10.5 • Plug-in Manager 2.0 (build 1188) **Note:** Refer to the OfficeScan Client/Server Edition 8.0/10.0/10.5/10.6 server documentation for minimum system requirements.

TABLE 1-1. System Requirements

COMPONENT	REQUIREMENTS
Policy Server	**Platform** • 2000 Server Family • 2003 Server Family • 2003 R2 Server Family • 2008 Enterprise Server • 2008 Data Center Server • 2008 R2 Enterprise Server • 2008 R2 Data Center Server • 2008 Core Server **Hardware** • 800-MHz Intel™ Pentium™ processor or equivalent • At least 1-GB of RAM • At least 40-MB of available disk space • 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 **Note:** When using IIS 7.0 or above for Master Server or Policy Server, make sure: • that **ISAPI Extensions** in Application Development, and **II6 management compatibility** are installed and enabled. • that **WebDAV** in Application Development is NOT installed.
Web browser	Internet Explorer 6.0 or above

Preparing Server Computer for Installation

This section provides the required information that you will need to prepare your server computer for the Trend Micro Mobile Security for Enterprise 7.1 installation.

General Prerequisites

1. **SQL Server installation**

   Install one of the following SQL Server versions:

   - Microsoft SQL Server 2005 (or Express edition)

     For the detailed SQL server 2005 installation procedure, refer to the following URL:

     http://msdn.microsoft.com/en-us/library/ms143516(v=SQL.90).aspx
   - Microsoft SQL Server 2008 (or Express edition)

     For the detailed SQL server 2008 installation procedure, refer to the following URL:

     http://msdn.microsoft.com/en-us/library/ms143219(v=SQL.100).aspx
   - Microsoft SQL Server 2008 R2 (or Express edition)

     For the detailed SQL server 2008 R2 installation procedure, refer to the following URL:

     http://msdn.microsoft.com/en-us/library/ms143219.aspx.

   Trend Micro recommends using SQL Server Authentication method for SQL Server instead of Windows Authentication. However, you can also configure Windows Authentication for SQL Server. Refer to *Using Windows Authentication for SQL Server* on page A-2 for details.
2. **Database creation**

   Create a database in SQL Server for Mobile Security 7.1.

   For the detailed SQL Server Management Studio installation procedure, refer to the following URL:

   http://msdn.microsoft.com/en-us/library/ms186312.aspx.
3. **Active Directory Service Account access rights**

Create Active Directory Service Account for Mobile Security 7.1 and assign it at least Read-Only access to Active Directory.

For the detailed Active Directory installation procedure, refer to the following URL:

http://technet.microsoft.com/en-us/library/cc757211(WS.10).aspx

4. **Router/Firewall Access Rules**

   Apply the following set of rules:

   - The Master Server and the Policy Server should be able to connect to the LDAP server for authentication.
   - The Master Server and the Policy Server should be able to connect to the remote SQL server, where the Trend Micro Mobile Security database is installed.
   - Configure the following two ports to establish a connection between the Master Server and the Policy Server:
     - 8189—the default port for SOAP connection. Allow inbound connection to Policy Server from Master Server on TCP port 8189.
     - 8190—the default port for socket connection. Allow inbound connection to Policy Server from Master Server on TCP port 8190.

     If you need to customize these port numbers, refer to *Configuring Policy Server Ports* on page A-3 for details.
   - All the mobile devices should be able to connect to the Policy Server.

iOS Support Prerequisite

1. **Certificate Authority**

   Install the Certificate Authority for iOS mobile devices. For the detailed Certificate Authority installation procedure, refer to the following URL:

   http://msdn.microsoft.com/en-us/library/ff720354.aspx

2. **Simple Certificate Enrollment Protocol (SCEP)**

   If you have set up SCEP on Windows Server 2003, install the SCEP Add-on for Certificate Services. Go to the following URL to download SCEP Add-on for Certificate Services:

   http://www.microsoft.com/downloads/details.aspx?FamilyID=9F306763-D036-41D8-8860-1636411B2D01&amp;displaylang=e&displaylang=en

   If you have set up SCEP on Windows Server 2008, install the Network Device Enrollment Service for Windows Server. Refer to the following URL for the installation and deployment procedure of Network Device Enrollment Service:

   http://technet.microsoft.com/en-us/library/ff955646(WS.10).aspx.

3. **Verifying system clocks**

   Make sure that the system clocks of SCEP server, Policy Server and the Master Server are set to the correct time.

4. **Modifying Policy Module properties for Certificate Authority**

   a. On the computer where Certificate Authority is installed, open the **Certification Authority** management console.

   b. Click **Policy Module** tab, and then click **Properties**.

   c. Select **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate**.

   d. Click **OK**.

5. **Apple Mobile Device Management (MDM) certificate**

   If you want to use the Mobile Device Management (MDM) feature on iOS4 or above mobile devices, obtain an Apple Push Notification Service (APNS) certificate from Apple.

6. **Router/Firewall Access Rules**

   Apply the following set of rules:

   - Configure the following ports:
     - TCP port 2195—Allow outbound connection from Policy Server to **Apple Push Notification Service** on TCP port 2195.
     - TCP port 2196—Allow outbound connection from Policy Server to **Apple Push Feedback Service** on TCP port 2196

    - Port 5223—For iOS devices, to receive a push notification from Apple's server, you must open port 5223, especially when connecting through a Wi-Fi network where port 5223 is blocked. However, if the mobile devices are on a 3G network, you do not need to open this port.
- iOS mobile devices should be able to connect to the Policy Server.
- Policy Server should be able to connect to SCEP server.
- iOS mobile devices should be able to connect to the SCEP server when registering to the Mobile Security server.

7. **SSL Server Certificate (Optional)**

   If you want use the secure-HTTP (HTTPS) service for the communication between mobile devices and Policy Server, obtain an SSL server certificate from a recognized Public Certificate Authority.

8. **Configuration Verification**

   To verify the server configuration for iOS mobile devices support, perform following:

   - For SCEP running on Windows Server 2008, access the following URLs from the Policy Server:
     - http://<SCEPServerIP>/certsrv/mscep_admin

       or

       https://<SCEPServerIP>/certsrv/mscep_admin

     Note: Replace **<SCEPServerIP>** with the actual SCEP server IP address in the URLs.

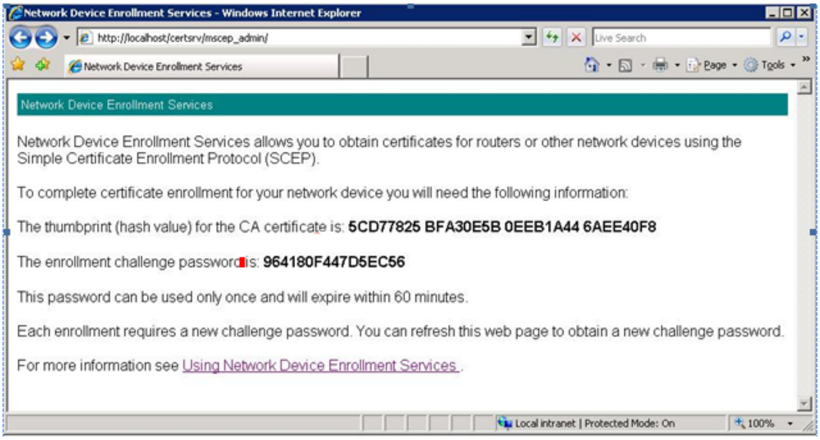
   - For SCEP running on Windows Server 2003: access the following URLs from the Policy Server:
     - http://<SCEPServerIP>/certsrv/mscep

       or

       https://<SCEPServerIP>/certsrv/mscep

     Note: Replace **<SCEPServerIP>** with the actual SCEP server IP address in the URLs.

If you see the Web page similar to the *Figure 1-3. Configuration Verification*, your server is configured correctly:


Network Device Enrollment Services - Windows Internet Explorer
http://localhost/certsrv/mscep_admin/
Live Search
Network Device Enrollment Services
Page
Tools
Local intranet | Protected Mode: On
100%

Network Device Enrollment Services

Network Device Enrollment Services allows you to obtain certificates for routers or other network devices using the Simple Certificate Enrollment Protocol (SCEP).

To complete certificate enrollment for your network device you will need the following information:

The thumbprint (hash value) for the CA certificate is: **5CD77825 BFA30E5B 0EEB1A44 6AEE40F8**

The enrollment challenge password is: **964180F447D5EC56**

This password can be used only once and will expire within 60 minutes.

Each enrollment requires a new challenge password. You can refresh this web page to obtain a new challenge password.

For more information see Using Network Device Enrollment Services .

FIGURE 1-3. Configuration Verification

Note: When iOS mobile device enrolls, it will be able to access the following URL: http://<SCEPServerIP>/certsrv/mscep or https://<SCEPServerIP>/certsrv/mscep.

The iOS mobile device only needs to connect to the SCEP server for enrollment, and does not require this connection for any further use.

BlackBerry Support Prerequisite

1. **BlackBerry Enterprise Server**

   Install the BlackBerry Enterprise Server (BES). Refer to the following URL for more information about BES 5.x:

   http://us.blackberry.com/apps-software/server/5/.

2. **BES User Administration Tool**

If you want to use the MDM feature on Blackberry devices, install BES User Administration Tool on the Master Server. Go the following URL to download the BES User Administration Tool:

https://swdownloads.blackberry.com/Downloads/entry.do?code=D736BB10D83A904AEFC1D6CE93DC54B8

3. **Router/Firewall Access Rule**

   Configure the following port:

   - TCP port 3101—Allow outbound connection from BES to connect BBI on TCP port 3101.

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:

- Master Server—hosts OfficeScan program and provides administrator management console.
- Policy Server—the server that handles communication between the Master Server and Mobile Device Agents (MDA)
- SMS Sender—mobile device that connects to the Policy Server to send SMS messages

WARNING! **If you are installing Master Server or Policy Server on Windows Server 2000, then you must first install Microsoft Data Access Component (MDAC). Otherwise, Trend Micro Mobile Security 7.1 may not be able to use the SQL Server properly.**

Installing Master Server

Before you can install the Master Server, make sure you have already installed the OfficeScan server version 8.0/8.0 SP1/10.0/10.0 SP1/10.5/10.5 SP1/10.5 SP2/10.6 and Plug-in Manager 1.0/2.0.

To install Master Server:

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, Policy 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 Master Server Web Console

You can access the management console for Master Server through the OfficeScan Web console.

To access the Master Server Web console:

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

Installing the Policy Server

Note: Trend Micro recommends installing the Master Server and the Policy Server on different computers.

Before you proceed with the Policy Server installation, make sure you have installed IIS Web server on the computer.

With IIS Web server, the Policy Server supports both HTTP and HTTPS connection types.

To install the Policy Server:

1. Log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.
3. Click **Administration** > **Policy Server Settings** > **Common Settings** and then click the download link to download Policy Server package to the computer on which you want to install the Policy Server.
4. Double-click the setup file to start the installation process.
5. Follow the on-screen instructions.
6. Select an IP address and type a service port number for the Policy Server The IP address and port number are used for the Policy Server to communicate with the Master Server (Trend Micro recommends selecting "ALL" for IP address.

Note: If the installation fails, make sure that the **ISAPI Extension** feature is installed for Internet Information Service (IIS). Also, make sure to install the Policy Server with the administrator privileges.

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 server
- update components from the Mobile Security server
- synchronize configuration with the Mobile Security server
- remote wipe the mobile device
- remote locate the mobile device
- remote lock the mobile device

You can install and connect up to 64 SMS senders to the Policy 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 Policy Server, you must configure the firewall rule to allow traffic on port 5721. Otherwise, the SMS sender cannot receive instructions from the Policy Server to send messages to mobile devices.**

To install an SMS sender:

1. On the Master 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 Policy Server and phone settings. In the **SMS Sender Config** screen, do the following:
   - Type the DNS name or IP address of the Policy 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 Master Server is unable to connect to the Internet, you need to install the Mobile Security server components on the Master 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 7.1 with a local update source:

1. On the Master Server, create a virtual directory "TmmsAu".

   Open the Internet Information Services (IIS) Manager screen and right-click **Default Web Site**. Then click **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 Master 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 1-21 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**).

Upgrading to Mobile Security v7.1

You can upgrade Mobile Security from version 7.0 to 7.1 on all management server components.

Note: If you upgrade from version 7.0 to 7.1 on a 64-bit operating system, make sure to disable the IIS OfficeScan Application Pool's 32-bit mode after completing the upgrade.

To disable the Office Scan Application Pool 32-bit mode:

1. Open the IIS management console, and click **Application Pools** in the left pane.
2. Select **OfficeScanAppPool** from the list in the center pane, and then click **Advanced Settings...** in the right pane. The **Advanced Settings** dialog box appears.
3. On the **Advanced Settings** dialog box, set **Enable 32-Bit Applications** to **False**.
4. Restart IIS.

Note: Before upgrading to Mobile Security 7.1, you must create a database in SQL server for Mobile Security 7.1.

If you only installed Mobile Security Management Module (MSMM) for Mobile Security 7.0, then do the following:

1. Upgrade MSMM to the Master Server for 7.1:
   a. Log on to the OfficeScan Web console and click **Plug-in Manager**. Then, click **Download** for Trend Micro Mobile Security. Mobile Security downloads the setup programs from the Trend Micro server.
   b. Click **Upgrade**.The setup program automatically uninstalls the previous version of MSMM and installs Mobile Security v7.1 Master Server.
2. Install the Policy Server. Refer to *Installing the Policy Server* on page 1-15 for the detailed procedure.

   Note: You must install the Master Server before the Policy Server.

3. Configure Policy Server settings. Refer to *Configuring Policy Server Settings* on page 1-24 for the detailed procedure.
4. Configure SMS senders. Refer to *Installing SMS Sender* on page 1-16 for the detailed procedure.

If you installed both Mobile Security Management Module (MSMM), and Mobile Security Comminication Module (MSCM) for Mobile Security 7.0, then do the following:

1. Upgrade MSMM to the Master Server for 7.1:
   a. Log on to the OfficeScan Web console and click **Plug-in Manager**. Then, click **Download** for Trend Micro Mobile Security. Mobile Security downloads the setup programs from the Trend Micro server.
   b. Click **Upgrade**.The setup program automatically uninstalls the previous version of MSMM and installs Mobile Security v7.1 Master Server.
2. Uninstall MSCM:
   a. Go to **Start** > **Control Panel** > **Programs and Features**
   b. Select Mobile Security Communication Manager program from the list, and then click **Uninstall**.
3. Install the Policy Server. Refer to *Installing the Policy Server* on page 1-15 for the detailed procedure.

   Note: You must install the Master Server before the Policy Server.

4. Configure Policy Server settings. Refer to *Configuring Policy Server Settings* on page 1-24 for the detailed procedure.
5. Configure SMS senders. Refer to *Installing SMS Sender* on page 1-16 for the detailed procedure.

Initial Server Setup

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

Initial server setup steps include:

1. *Registering the Product* on page 1-21
2. *Configuring Database Settings* on page 1-23
3. *Configuring Active Directory (AD) Settings* on page 1-23
4. *Configuring Common Policy Server Settings* on page 1-24
5. Installing Certificate Authority (CA) and Simple Certificate Enrollment Protocol (SCEP) server. Refer to *iOS Support Prerequisite* on page 1-9.
6. *Managing Apple Push Notification Service Certificate* on page 1-27
7. *Configuring iOS Policy Server Settings* on page 1-25
8. *Configuring BlackBerry Policy Server Settings* on page 1-26
9. *Configuring Notification Settings* on page 1-27
10. *Configuring Error Message Notification* on page 1-28

Note: You must complete the initial server setup for the Mobile Security server before you continue to install Mobile Device Agent on mobile devices.

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 server 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 data protection module is included with Mobile Security server. Please consult your local Trend Micro sales representative for more information.

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

If the data protection module is activated on the Mobile Security server and the data protection policies are configured, Mobile Device Agents will install the data protection module on the supported mobile devices after product registration is successful.

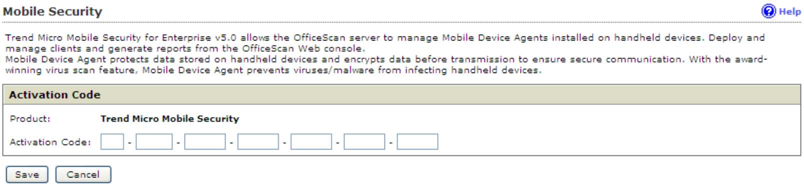
Activation Code Format

An activate code displays in the following format:

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

To register Mobile Security server:

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**.



Mobile Security

Trend Micro Mobile Security for Enterprise v5.0 allows the OfficeScan server to manage Mobile Device Agents installed on handheld devices. Deploy and manage clients and generate reports from the OfficeScan Web console.
Mobile Device Agent protects data stored on handheld devices and encrypts data before transmission to ensure secure communication. With the award-winning virus scan feature, Mobile Device Agent prevents viruses/malware from infecting handheld devices.

Activation Code

Product: Trend Micro Mobile Security

Activation Code: [ ] - [ ] - [ ] - [ ] - [ ] - [ ] - [ ]

FIGURE 1-4. 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 7.1 Advanced Edition has been activated." if product registration is successful.

Configuring Database Settings

Note: You must create a database in SQL server before configuring it in Mobile Security 7.1. While configuring, use the same database name in SQL server and Mobile Security 7.1.

To configure Database Settings:

1. Log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.
3. Click **Administration** > **Database Settings**.
4. Type the server name or IP address, your username, password and the database name.
5. Click **Save**. The **Summary** screen for Mobile Security displays.

Configuring Active Directory (AD) Settings

Trend Micro Mobile Security 7.1 enables you to configure user authorization based on the Active Directory (AD). You can also add mobile devices to the device list using your AD.

To configure Active Directory Settings:

1. Log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.
3. Click **Administration** > **Active Directory Settings**.
4. Type the host name or its IP address, its port number, your domain username and your password.
5. Click **Save**. The **Summary** screen for Mobile Security displays.

Configuring Policy Server Settings

Mobile Security 7.1 provides the following two types of settings:

- **Public Settings for Mobile Devices**—used for communication between Policy Server and mobile devices. Mobile devices only need to connect to the Policy Server. If the Master Server and the Policy Server are installed on the same computer, the mobile devices should be able to communicate to that computer.
- **Internal Settings for Management Module**—used for communication between Policy Server and Master Server, and uses port 8189 for Simple Object Access Protocol (SOAP) communications.

Configuring Common Policy Server Settings

To configure Common Policy Server Settings:

1. Log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.
3. Click **Administration** > **Policy Server Settings**.
4. On the **Common Settings** tab, fill all the fields with the relevant information.

Note: Consider the following while configuring Common Policy Server Settings:

- **Public Settings for Mobile Devices:**
  - If you do not select **HTTPS port** in **Public Settings for Mobile Devices**, the mobile devices will use HTTP port to communicate with the Policy Server.
  - To use HTTPS port to communicate with the Policy Server, you will need to upload the SSL certificate to Mobile Security:

    i. Click **Administration** > **Certificate Management**.

    ii. Click **Add**, select the certificate, and then click **Save**.
  - iOS 5.x, mobile devices support HTTPS only. Therefore, if you want to manage iOS 5.x mobile devices, select HTTPS port.
  - For basic security model (single server installation), the default ports of Policy Server and Master Server are as follows:
    - HTTP port: 8080
    - HTTPS port: 4343

        - For enhanced security model (dual server installation), the default ports of Policy Server are as follows:
            - HTTP port: 80
            - HTTPS port: 443
    - **Internal Settings for Management Module:**
        - Use the default port number **8189** for SOAP connection. If you need to customize this port number, refer to *Configuring Policy Server Ports* on page A-3 for details.

5. Click **Save**.

Configuring iOS Policy Server Settings

To configure iOS Policy Server Settings:

1. Log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.
3. Click **Administration** > **Policy Server Settings**.
4. On the **iOS Settings** tab, fill the fields with the following information:
    - Simple Certificate Enrollment Protocol (SCEP) Settings
        - **SCEP user URL:**

          http://SCEP_IP/certsrv/mscep

          -or-

          https://SCEP_IP/certsrv/mscep
        - **SCEP admin URL:**
            - For Windows Server 2008:

              http://SCEP_IP/certsrv/mscep_admin

              -or-

              https://SCEP_IP/certsrv/mscep_admin
            - For Windows Server 2003:

              http://SCEP_IP/certsrv/mscep

              -or-

              https://SCEP_IP/certsrv/mscep

  - **User account:** <login user name>
  - **Password:** <login password>
  - **Certificate name:** <a name for certificate>
  - **Subject:** **`O=TrendMicro,CN=Enroll`**
- Apple Push Notification service (APNs) Settings
  - **Certificate type:** Select your certificate type.
  - **Certificate:** Select APNS certificate from the dropdown list, or upload a new one.
- Profile Signing Credential
  - **Credential:** Select a certificate for signing credential from the dropdown list, or upload a new one.

5. Click **Save**.

Configuring BlackBerry Policy Server Settings

Note: Before configuring BlackBerry Policy Server settings, you must install **brk-besuseradminclient** command tool on the Mobile Security Master Server.

To find BlackBerry Command Tool path:

1. Log on to the BlackBerry Administration Service**.**
2. From **Servers and components** menu, click **BlackBerry Solution topology** > **BlackBerry Domain** > **Component View**.
3. On the right pane, you can see the BlackBerry Enterprise Server instance name.

To configure BlackBerry Policy Server Settings:

1. Log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.
3. Click **Administration** > **Policy Server Settings**.
4. On the **BlackBerry Settings** tab, fill all the fields with the relevant information.
5. Click **Save**.

Managing Apple Push Notification Service Certificate

Note: If you have already uploaded an APNS certificate from **Apple Push Notification service (APNs) Settings** on iOS device, then you do not need to upload it again in Certificate Management.

To manage Apple Push Notification certificate:

1. Log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.
3. Click **Administration** > **Certificate Management**.
4. Click **Add**, select the Apple Push Notification Server certificate from the hard disk, and then click **Save**.

Configuring Notification Settings

You may configure the notification source to send out the notification email message to the administrators.

To configure Notification Settings:

1. Log on to the Office Scan Web console and click **Plug-in Manager**.
2. Click **Manage Program**.
3. Click **Notification > Settings**.
4. You can now configure SMTP server settings and the SMS sender list for outgoing notifications:
    - To configure SMTP server settings for email notification messages: type the **From** email address, the SMTP server IP address and its port number. If the SMTP server requires authentication, select **Authentication**, and then type the username and password.
    - To configure text message notifications: in the **SMS Sender Settings** section, click **Add**, type the phone number of an SMS sender on the pop-up that appears, and then click **Save**. The SMS sender list displays the phone number that you added. 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 Policy Server.

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 Policy Server.**

Configuring Error Message Notification

To configure notifications sent to the administrators:

1. Log on to the Office Scan Web console and click **Plug-in Manager**.
2. Click **Manage Program**.
3. Click **Notification > To Administrator**.
4. Type the email address, subject and the message, and then click **Save**.

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* on page 2-2
- *Installing Mobile Device Agent* on page 2-3
- *Installing Mobile Device Agent* on page 2-3
- *Using the Encryption and Password Module* on page 2-12

Planning Mobile Device Agent Installation

Note: Make sure the mobile devices can connect to the Policy Server 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
Android 2.1 or above	10	8

Note: For iOS mobile devices, Mobile Security supports iOS 4.x and above.
For Blackberry mobile devices, Mobile Security supports BES 5.x.

Note: iOS and BlackBerry mobile devices does not require any Mobile Security client software (Mobile Device Agent) installation.

Mobile Device Agent Installation Methods

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

- Installation through SMS messages or email—sends SMS messages or email with Mobile Device Agent installation URL to mobile devices or users' email addresses. Users need to access the URL in the SMS message or email, and then register the mobile device with the Policy Server. You need to install the SMS senders if you want to send SMS notification messages.
- Memory card—for Symbian or Windows platforms, download the setup file from the Master Server and copy the extracted files to a memory card. Once you insert the memory card into a mobile device, Mobile Device Agent installation is automatic.

Note: Memory card installation method is not available if you want to re-install or upgrade Mobile Device Agent for Mobile Security for Enterprise 7.1 on Symbian devices. In this case, you should use the manual installation method.

- 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 Policy Server. For detailed instructions on manual installation and registration, refer to *Launching the Setup File Manually* on page 2-7 or the User's Guide for your mobile device platform.

Installing Mobile Device Agent

To use the data protection 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 data protection module on Windows Mobile devices will not work if the built-in password security or the memory card encryption feature is enabled.

Silent Installation Using Email or SMS Notifications

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

- *Configuring Notification Settings* on page 1-27
- *Configuring Installation Message* on page 2-4
- *Configuring the Mobile Device List* on page 2-5

Configuring Installation Message

To initiate silent Mobile Device Agent installation, Mobile Security sends an email and/or a text message to notify mobile devices to download and install Mobile Device Agent.

Users can open the text message and download the Mobile Device Agent setup package by accessing the URL included in the email or the text message. The Mobile Device Agent setup package will automatically fill the server IP and port number, while users will need to type the device name, domain name and password to register.

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

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 **Notification** > **To User**.
4. Type the email and/or the text message in the related text box(es).

   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.

   Note: The email notification only sends the download link for downloading client setup files, and will not automatically fill the server IP address and port number in the register screen.

5. Click **Save**.

Configuring the Mobile Device List

Configure the mobile device list on the Mobile Security server 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 using a memory card, the Mobile Security server will automatically add Mobile Device Agent information to the list after the device is registered to the Mobile Security Management Module.

To add a mobile 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**.
5. Select **Add a device** and do one of the following:
   - Search and add the user from the active directory.
   - Configure the following fields for manual addition:
     - **Phone number**—type the phone number of a mobile device. To ensure that the mobile device can receive notification messages successfully from an SMS sender, you may type the country code (1-5 digits long). You do not have to type the international direct dialing prefix.
     - **Email**—type the user email address to send notification mail.
     - **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. 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 server 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 server, 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 registers to the Mobile Security server. 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 (Symbian and Windows)

You can use a memory card to automatically install Mobile Device Agent on mobile devices. You need to download the setup file from the Mobile Security server 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 server:

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 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. Register to the Mobile Security Management server. Select an AP that your mobile device use to connect to the Policy 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 server.

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 server.

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 server:

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. Select the setup file and 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 using computer software.

   - 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`
   - Android 2.1 or above:

     `TmmsSuite.apk`

   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://<OfficeScan_ServerIP:Port>/officescan/PLS_TMMS_CGI/cgiOsmaProvision.dll

   or

   https://<OfficeScan_ServerIP: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

   or

   https://<Public_Address:Port>/officescan/PLS_TMMS_CGI/cgiOsmaProvision.dll

Note: 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
Android: TmmsSuite.apk
Symbian S60 3rd/5th on Nokia mobile device:
MobileSecurity_S60.sis
```

To manually install Mobile Device Agent on Windows or Symbian 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:
   - For Windows Mobile: `\Program Files\Trend Micro\Mobile Security\`
   - For Symbian: `C:\system\data\mobilesecurity\` (Symbian OS requires a 3rd-party file explorer to access this directory.)
4. Restart the mobile device. After the restart is complete, the **Device name**, **Host name or IP address**, and **Port number** fields in the **Register** screen displays the valid information.

Manual Registration

You will need to manually register Mobile Device Agent to the Policy Server if you install Mobile Device Agent manually or if the automatic registration process fails.

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

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, HTTP or HTTPS port number of the Policy Server, your domain user name and its password. Click **Register**.
3. After the registration is completed, view the license information in the About screen (**Menu** > **About**) on Windows and Symbian mobile devices and on the summary screen on Android mobile devices. You can also see the device status on the Mobile Security server.

Note: The registration process may take several minutes.

iOS Provisioning

To be able to manage iOS mobile device from the Master Server, you must install a provisioning profile on the mobile device. This provisioning profile must identify you (through your development certificate) and your device (by listing its unique device identifier).

Note: Before provisioning an iOS device, the user must have a valid Active Directory user account.

To install provisioning profile on iOS mobile device:

1. On the iOS mobile device, open the Safari Web browser, and go to the following URL:

   http://<Public_Address:Port>/officescan/PLS_TMMS_CGI/cgiOsmaProvision.dll

   or

   https://<Public_Address:Port>/officescan/PLS_TMMS_CGI/cgiOsmaProvision.dll

   The **Authentication Required** pop-up dialog box appears.

2. Type your domain accout and password, and then tap **Log In**. The **Install Profile** screen displays.
3. Tap **Install**, and then tap **Install Now** on the confirmation pop-up dialog box.
4. If the mobile device requires a passcode, then type your passcode on the **Enter Passcode** screen that appears, and then tap **Done**. The **Installing Profile** screen appears.
5. Tap **Install** on the **Warning** confirmation screen. The profile installation process begins.After the process is completed, the **Profile Installed** screen displays.
6. Tap **Done**.-

To uninstall provisioning profile from iOS mobile device:

1. On the iOS mobile device, go to **Settings** > **General** > **Profiles**.
2. Select **MDM Enrollment Profile**, and then tap **Remove**. If you have configured the device lock password, type the password to uninstall the provisioning profile.

Using the Encryption and Password Module

The encryption and password 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 server
- the encryption and password license is included in the product license, and encryption and password is enabled
- the encryption module supports the mobile device platform

Note: The encryption in Mobile Security for Enterprise 7.1 supports Windows Mobile 5/6 operating system, but does not support Symbian S60 3rd/5th, Android, iOS and BlackBerry operating systems.

- card encryption function is 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 server To register the Mobile Device Agent, refer to *Manual Registration* on page 2-10.
2. Restart the mobile device to activate the encryption and password 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.

Appendix A

Optional Configurations

This appendix provides optional configuration procedures that you can perform while installing Trend Micro Mobile Security.

This chapter contains the following sections:

- *Using Windows Authentication for SQL Server* on page A-2
- *Configuring Policy Server Ports* on page A-3
- *Increasing Server Scalability* on page A-4

Using Windows Authentication for SQL Server

Trend Micro recommends using SQL Server Authentication method for SQL Server instead of Windows Authentication. However, you can also configure Windows Authentication for SQL Server.

To use Windows Authentication:

1. Make sure that the Master Server, Policy Server and the database are in the same domain.
2. On the Master Server, open **`TmDatabase.ini`** in a text editor (located in `C:\Program Files\Trend Micro\OfficeScan\Addon\Mobile Security\`), and make the modifications as follows:

```
[Database]

ServerAddress=10.64.66.221\sqlexpress

DatabaseName=TMMS_JAMES_1111

UserName=!CRYPT!105152456BB074F23053C5A4F0C

Password=!CRYPT!105152456BB074F23053C5A4F0C

ConnectionStringFormat=Provider=sqloledb;Data
Source=%server%;Initial Catalog=%database%;Integrated
Security=SSPI;
```

3. Copy the modified **`TmDatabase.ini`** file to the Policy Server setup directory (located at `C:\Program Files\Trend Micro\Mobile Security\PolicyServer`)
4. On the Master Server, open Windows services, and double-click **OfficeScan Plug-in Manager.**
5. On the **Log On** tab, select **This account:** and type the account name that will access the database, and its password in **Password** and **Confirm password** fields, and then click **OK**.
6. Right-click on the **OfficeScan Plug-in Manager** in the services list, and then click **Restart**.
7. On the Master Server, repeat steps 4 to 6 for the following services:

- Mobile Security Management Module Service
- Mobile Security Monitor Service
- Mobile Security Management Module BlackBerry Service

8. On the Policy Server, repeat steps 4 to 6 for the following service:
   - Mobile Security Management Module IOS Service
   - Mobile Security Communication Module (MSCM) server
9. Configure database settings on OfficeScan Web Console:
   a. Log on to the OfficeScan Web console.

   b. Click **Plug-in Manager** in the main menu.

   c. Click **Administration** > **Database Settings**.

   d. Type the server IP address and the database name as you configured in step 2, and leave the **User name** and **Password** fields blank.

   e. Click **Save**.

Configuring Policy Server Ports

Trend Micro Mobile Security 7.1 enables to you to customize the Policy Server ports that it uses to establish the connection with the Master Server.

To configure Policy Server ports:

1. Configure socket and SOAP ports on the Master Server:
   a. On the Master Server, open `TmDatabase.ini` in a text editor (located in `C:\Program Files\Trend Micro\OfficeScan\Addon\Mobile Security\`).

   b. Modify the values of `omsm_svr_port` for SOAP port:, and `PolicyServerIPCPOrt` for the socket port.

   c. Save and then close `TmDatabase.ini` file.

   d. Open Windows services, and right-click **OfficeScan Master Service**, and then click **Restart**.
2. Configure socket and SOAP ports on the Policy Server:

a. On the Policy Server, open `omsm_srv.ini` in a text editor (located in `C:\Program Files\Trend Micro\Mobile Security\PolicyServer\`).

b. Modify the values of `omsm_soap_port` for SOAP port, and `[sockIPC] port`for the socket port.

c. Open Windows services, and restart the following services:

- **Mobile Security Communication Module (MSCM) Server**

Mobile Security Mangement Module IPC proxy service

Increasing Server Scalability

Depending on your requirements, you can increase the server scalability and improve server performance.

To increase server scalability and improve server performance:

1. Open the **Internet Information Services (IIS) Manager**, and select the server on which you want to perform this procedure.
2. Click **Application Pools** in the left pane, select the AppPool where Mobile Security is installed from the list in the center pane, and then click **Advanced Settings...** in the right pane. The **Advanced Settings** dialog box appears.
3. On the **Advanced Settings** dialog box, make the following changes:
   - Change the value of the parameter **Queue Length** to `65535`.
   - Change the value of the parameter **Maximum Worker Processes** to `5` or more.
4. After making the changes, Click **OK**, and close the **Internet Information Services (IIS) Manager**.
5. Open Windows **Command** prompt, and then:
   - type the following command to change the value of IIS concurrent request limit to 100000:

     ```
     c:\windows\system32\inetsrv\appcmd.exe set config /section:serverRuntime /appConcurrentRequestLimit:100000
     ```

Note: To verify this change, open file ***`applicationHost.config`*** by typing command file **%systemroot%\System32\inetsrv\config\applicationHost.config** in the Command prompt, and then verify the value of parameter ***serverRuntime appConcurrentRequestLimit***, which should be **`100000`**.

- type the following command to change IIS concurrent request limit to 100000 in the Windows registry:

  reg add HKLM\System\CurrentControlSet\Services\HTTP\Parameters /v MaxConnections /t REG_DWORD /d 100000