TREND MICRO™

8.0 Mobile Security™ Service Pack 1

Installation and Deployment Guide

Comprehensive security for enterprise handhelds

Endpoint Security

Release Date: September 2012

Document Part No.: TSEM85685/120925

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: Planning Server Installation

Chapter 2: Preparing Server Computer for Installation

Chapter 3: Installing and Removing Server Components

Chapter 4: Configuring Server Component

Chapter 5: Handling Mobile Device Agent

Appendix A: Firewall Ports Configurations

Appendix B: Optional Configurations

Appendix C: Generating and Configuring APNs Certificate

Appendix D: Generating and Configuring SSL Certificate

Preface

Preface

Welcome to the Trend Micro™ Mobile Security for Enterprise 8.0 SP1 Installation and Deployment Guide. This guide assists administrators in deploying and managing Mobile Security for Enterprise 8.0 SP1. 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 8.0 SP1. 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.
- **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

Planning Server Installation

This chapter assists administrators in planning the server components for Trend Micro Mobile Security for Enterprise 8.0 SP1.

This chapter contains the following sections:

Network Planning

Mobile Security for Enterprise 8.0 SP1 consists of the following four components:

- Management Server
- Communication Server
- SMS Senders or SMS Gateway (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 Communication Server and Management Server on the same computer. *Figure 1-1* shows where each Mobile Security component resides in a typical Basic Security Model.

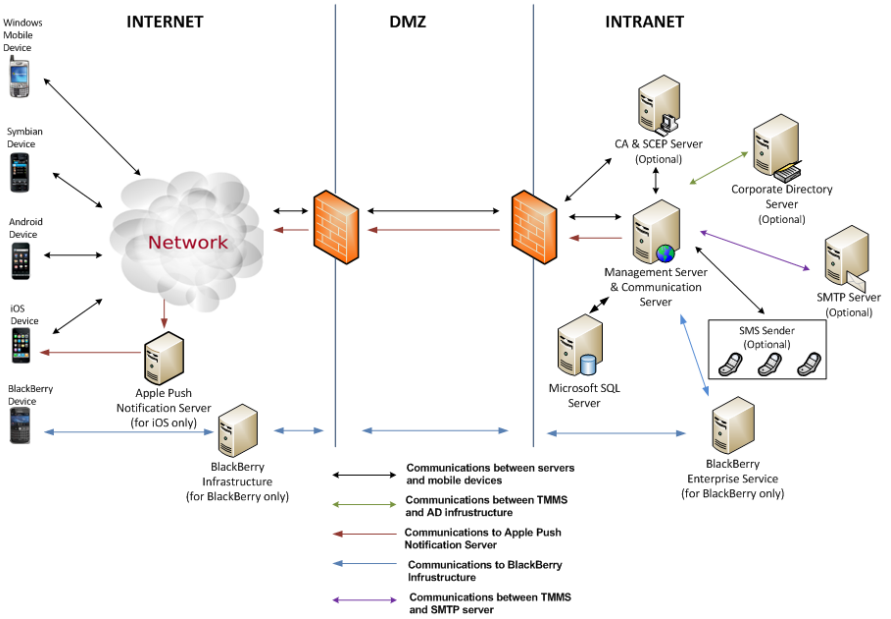

FIGURE 1-1. Basic Security Model

Enhanced Security Model (Dual Server Installation)

The Enhanced Security Model supports the installation of Communication Server and Management 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.**

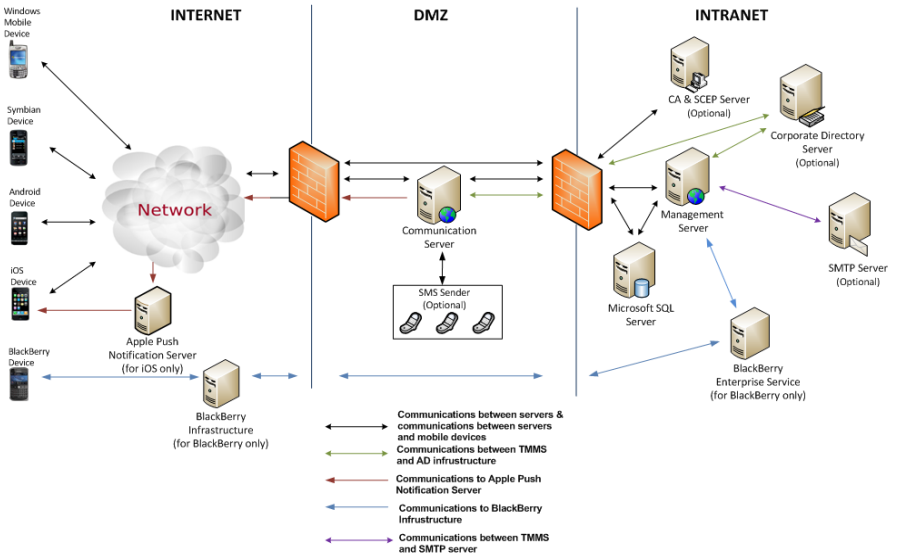

FIGURE 1-2. Enhanced Security Model

Management Server

The Management Server is a plug-in program that enables you to control Mobile Device Agents from the OfficeScan Web console. Once mobile devices are registered, you can configure Mobile Device Agent policies and perform updates.

Communication Server

The Communication Server handles communications between the Management Server and Mobile Device Agents. The Communication Server allows the Management Server to manage Mobile Device Agents outside the corporate intranet. Mobile Device Agents can connect to the public IP address of the Communication Server.

You can use the OfficeScan Web console to configure policies for the Communication Server.

SMS Gateway and SMS Sender

You can use either SMS Gateway or SMS Sender to send SMS messages to the users according to your requirements and network configuration.

Note: By default, Mobile Security is configured to use SMS Sender to send SMS messages. However, you can change the default configuration. Refer to the topic *Configuring Notification Settings* in Administrator's Guide for details.

- The **SMS Gateway** is a service that can send SMS messages to the users.
- **SMS senders** are designated mobile devices connected to the Communication Server over WLAN connections or ActiveSync (version 4.0 or above). An SMS sender receives commands from server and relays them to mobile devices via SMS text messages.

SMS text messages may be used to notify mobile devices to:

- download and install Mobile Device Agent
- register Mobile Device Agent to the Mobile Security server
- update the Mobile Device Agent components from the Mobile Security server
- wipe, lock or locate the remote mobile device
- synchronize policies with the Mobile Security server

Mobile Device Agent

Install the Mobile Device Agent on supported platforms using one of the installation methods—SMS message notification, email notification, memory card and manual installation. The Mobile Device Agent provides seamless protection against malware,

unwanted SMS/WAP-Push messages or network traffic. Users will enjoy the benefits of real-time scanning, firewall protection and data encryption when sending/receiving messages and opening files on the mobile devices.

System Requirements

Review the following requirements before installing each Mobile Security component in your network.

TABLE 1-1. System Requirements

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

TABLE 1-1. System Requirements

COMPONENT	REQUIREMENTS
Communication Server	**Platform** • Windows 2003 Server Family • Windows 2003 R2 Server Family • Windows 2008 Server Family • Windows 2008 R2 Server Family **Recommended Platform** • Windows Server 2008 R2 Enterprise Edition • Windows Server 2008 Enterprise Edition SP1 • Windows Server 2003 R2 Enterprise Edition • Windows Server 2003 Enterprise Edition • Windows Server 2008 Standard Edition • Windows Web Server 2008 Edition SP1 **Hardware** • 1-GHz 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
SQL Server	• Microsoft SQL Server 2005 • Microsoft SQL Server 2005 Express Edition • Microsoft SQL Server 2008 • Microsoft SQL Server 2008 Express Edition • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2008 R2 Express Edition
Web Server for Communication Server	• Microsoft Internet Information Server (IIS) 6.0/7.0/7.5 **Note:** When using IIS 7.0 or above for Management Server or Communication Server, make sure: • that **ISAPI Extensions** in Application Development, and **IIS6 management compatibility** are installed and enabled. • that **WebDAV** in Application Development is NOT installed. **Note:** Trend Micro Mobile Security does NOT support Apache Web server.
Web browser	Internet Explorer 7.0 or above

Chapter 2

Preparing Server Computer for Installation

This chapter provides the required information that you will need to prepare your server computer for the Trend Micro Mobile Security for Enterprise 8.0 SP1 installation.

This chapter contains the following sections:

General Prerequisites

You need to perform the following to prepare your server computer for the installation for all the mobile device platforms.

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 2008/2008 R2 (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

   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 B-2 for details.

2. **Active Directory Service Account access rights (Optional)**

   Note: You only need to perform this step if you plan to use Active Directory for user authentication or import users from active directory. Otherwise, skip this step.

   Create Active Directory Service Account for Mobile Security 8.0 SP1 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

3. **Router/Firewall Access Rules**

   Apply the following set of rules:

   - If you plan to use active directory for user authentication or import users from active directory, the Management Server and the Communication Server should both be able to connect to the Corporate Directory server.
   - The Management Server and the Communication Server should both 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 Management Server and the Communication Server:
     - 8189—the default port for SOAP connection. Allow inbound connection to Communication Server from Management Server on TCP port 8189.
     - 8190—the default port for socket connection. Allow inbound connection to Communication Server from Management Server on TCP port 8190.

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

iOS Support Prerequisite

1. **Certificate Authority (Optional)**

   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

Note: Certificate Authority is required if you want to use SCEP for iOS mobile devices. If you do not want to use SCEP, you do not need to install the Certificate Authority.

---

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

Note: If you do not want to use SCEP for iOS mobile devices, you will need to disable it in Communication Server Settings after you have installed the Management Server and the Communication Server. Refer to *Configuring iOS Communication Server Settings* on page 4-8 for the procedure.

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://esupport.trendmicro.com/solution/en-us/1060187.aspx

or

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

Note: If you want to use SCEP, Trend Micro recommends using it on Windows Server 2008.

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://esupport.trendmicro.com/solution/en-us/1060258.aspx

or

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

3. **System clocks verification**

   Make sure that the system clocks of SCEP server, Communication Server and the Management 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 Push Notification server (APNs) 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. Refer to *Appendix C, Generating and Configuring APNs Certificate* starting on page C-1 for the detailed procedures.

6. **Router/Firewall Access Rules**

   Apply the following set of rules:

   - iOS mobile devices should be able to connect to the Communication Server.
   - If you are using SCEP, then:
     - Communication Server should be able to connect to SCEP server.
     - iOS mobile devices should be able to directly connect to the SCEP server when registering to the Mobile Security server.
   - Configure the following ports:
     - TCP port 2195—Allow outbound connection from Communication Server to **Apple Push Notification Service** on TCP port 2195. The hostname of Apple Push Notification Service is **`gateway.push.apple.com`**.
     - 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.

7. **SSL Server Certificate (for HTTPS communication)**

   If you want to use the secure-HTTP (HTTPS) service for the communication between mobile devices and Communication Server, obtain an SSL server certificate from a recognized Public Certificate Authority or generate a private SSL server certificate and install it on the Communication Server. Refer to *Appendix D, Generating and Configuring SSL Certificate* starting on page D-1 for the detailed procedures.

iOS 5.x, mobile devices only support HTTPS. Therefore, if you want to manage iOS 5.x mobile devices, you must use HTTPS to communicate with the Communication Server, and configure the SSL certificate on the Communication Server.

Note: Since only the Communication Server communicates with the mobile devices, you do not need to configure the SSL certificate on the Management Server.

8. **Configuration Verification for SCEP server (Optional)**

If you have setup SCEP for iOS mobile devices, perform the following to verify the server configuration:

- For SCEP running on Windows Server 2008, access the following URLs from the Communication Server:
  - http://<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 Communication Server:
  - http://<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 2-3. Configuration Verification*, your server is configured correctly:

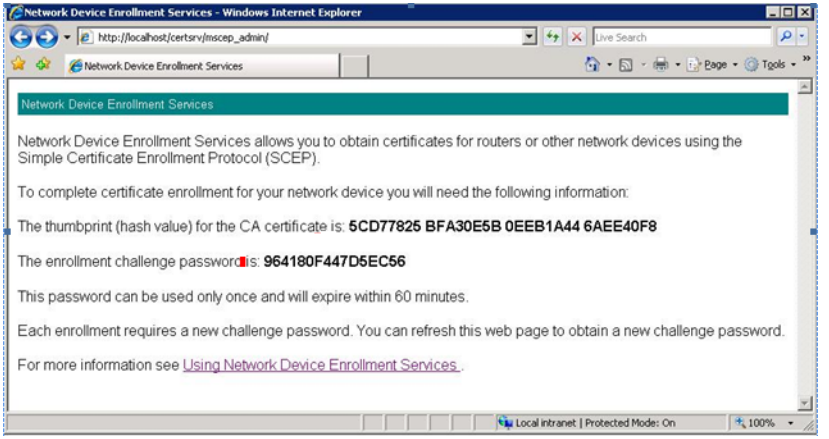

FIGURE 2-3. Configuration Verification

Note: When iOS mobile device enrolls, it will be able to access the following URL: http://<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 URLs for more information about BES 5.x:

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

   and

   http://docs.blackberry.com

2. **BES User Administration Tool**

   If you want to use the Mobile Security for Blackberry devices, install BES User Administration Tool on the Management Server.

   To download the BES User Administration Tool:

   a. Go the following URL:

      http://us.blackberry.com/support/downloads/

   b. From the list of **Business software**, click **BlackBerry Enterprise Server Resource Kit**, and then read the instructions on the Web page to download the **BlackBerry Enterprise Server User Administration Tool v5.0 Service Pack 2** from the **BlackBerry Enterprise Server Resource Kit v5.0 Service Pack 2**.

3. **BlackBerry mobile device activation**

   You must activate the BlackBerry mobile device before you are able to manage them using Mobile Security. Refer to the following URL for the details:

   http://docs.blackberry.com

4. **Router/Firewall Access Rule**

   Configure the following port:

   - TCP port 3101—Allow outbound connection from BES to connect BlackBerry Infrastructure (BBI) on TCP port 3101.

Chapter 3

Installing and Removing Server Components

This chapter guides the administrators in installing Trend Micro Mobile Security for Enterprise 8.0 SP1 server components. This chapter also guides on how to remove the server components.

This chapter contains the following sections:

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 determine the Mobile Security server components you want to install.

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

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

---

Note: The Management Server and Communication Server do not support the installation on Windows Server 2000.

Installing Management Server

Before you can install the Management Server, make sure you have already installed the following:

- Microsoft IIS Web server for OfficeScan server
- OfficeScan server version 10.0/10.5/10.6 and Plug-in Manager 1.0/2.0.

To install Management 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, Communication 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.

Note: Mobile Security requires Java Runtime Environment (JRE) to upload .apk file from the Application Management module on the Management Server. The JRE is automatically installed with the installation of the Management Server. However, if the computer where you have installed the Management Server already has the JRE installed, then the Management Server setup will not install JRE. If the existing JRE version is older than 1.6, then you will need to manually uninstall JRE, and install the version 1.6 or above.

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.

You only need to register Mobile Security server on the Management 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.

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**.

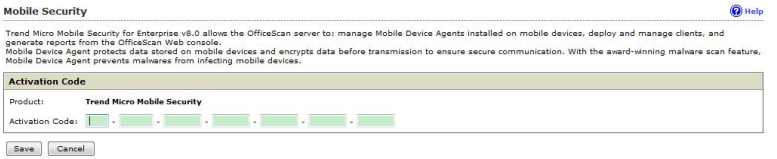

FIGURE 3-4. Registering Mobile Security after installation

4. Verify that product registration is successful. Click **Dashboard** to display the Dashboard screen. You should see the message "Trend Micro Mobile Security 8.0 SP1 has been activated." if product registration is successful.

After the registration is complete, the **Getting Started** screen as shown in *Figure 3-5* displays and guides you through the steps to complete the initial settings.

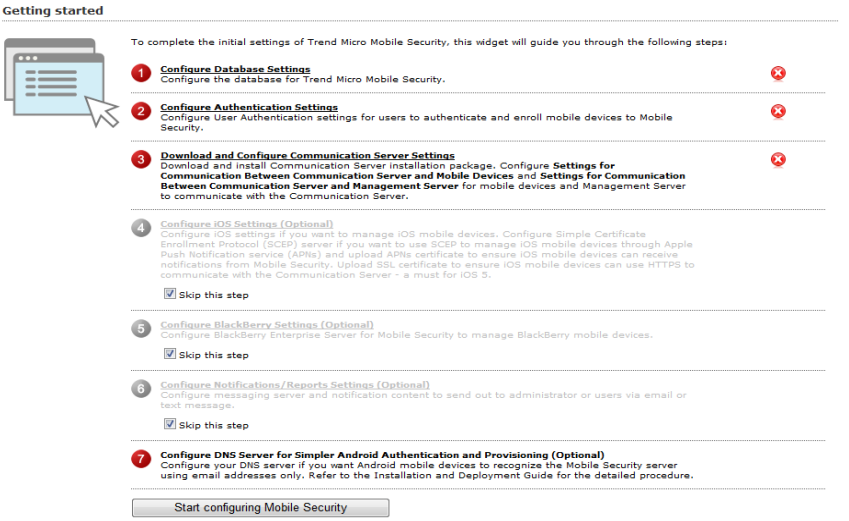

FIGURE 3-5. Getting Started screen

Accessing the Management Server Web Console

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

To access the Management Server Web console:

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

Accessing Management Server Web Console Using Internet Explorer 9 with IIS version 6

If you are using IIS version 6 for Management Server, you need to configure the correct Multimedia Internet Mail Extensions (MIME) type for Cascading Style Sheets (CSS) to display the Management Server Web console correctly.

To configure the MIME type for CSS in IIS 6:

1. Open the Internet Information Services (IIS) Manager screen and then right-click **OfficeScan** > **officescan** > **console** and click **Properties**. The **console Properties** pop-up window displays.
2. On the **HTTP Headers** tab, click **MIME Types**, and then click **New**.
3. In the **Extension** text filed, type `.css` and in the **MIME type** text field, type `text/css`, and then click **OK**.
4. **Click OK** on the **MIME Types** pop-up window and then on the **console Properties** pop-up window.

Installing Communication Server

Note: Before you proceed with the Communication Server installation, make sure you have installed IIS Web server on your computer.

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

To install the Communication Server:

1. Log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.

3. Click **Administration** > **Communication Server Settings** > **Common Settings** and then click the download link to download Communication Server package to the computer on which you want to install the Communication 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 Communication Server. The IP address and port number are used for the Communication Server to communicate with the Management 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 Communication Server with the administrator privileges.

Installing SMS Sender

SMS sender is a Windows Mobile device that your require to install only if you want to send SMS text messages to push notifications to users from the Mobile Security server

Note: If you do not use SMS Sender, only the remote lock and remote wipe instructions will not be pushed to the Windows Mobile devices. However, all other features will work as normal. Also, if you do not use SMS Sender, all the features of Mobile Security will work as normal for iOS, Android, BlackBerry and Symbian mobile devices.

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 Communication 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** Communication Server**, you must configure the firewall rule to allow traffic on port 5721. Otherwise, the SMS sender cannot receive instructions from the** Communication Server **to send messages to mobile devices.**

To install an SMS sender:

1. On the Management Server, copy the setup file from the folder `\OfficeScan\Addon\Mobile Security\AgentPackage\SmsSender` to a memory card for the supported Windows Mobile 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 Communication Server and phone settings. In the **SMS Sender Config** screen, do the following:
   - Type the DNS name or IP address of the Communication 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 Management Server is unable to connect to the Internet, you need to install the Mobile Security server components on the 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 8.0 SP1 with a local update source:

1. On the Management Server, do the following to 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.

   The "TmmsServerAu" folder should contain ***OSCE_AOS_COMP_LIST.zip***, ***OSCE_PLS_TMMS.zip***, ***OSCE_PLS_TMMS_Install.zip*** and ***server.ini***.

   The folder "TmmsClientAu" should contain mobile client applications and ***server.ini***.

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 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 3-3 for more information. After product registration is completed successfully, the **Dashboard** 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 v8.0 SP1

You can upgrade Mobile Security from version 7.0/7.1 to 8.0 SP1 on all management server components.

Note: If you upgrade from version 7.0 to 8.0 SP1 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 OfficeScan 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.

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

1. Upgrade MSMM to the Management Server for 8.0 SP1:
   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 8.0 SP1 Management Server.
2. Install the Communication Server. Refer to *Installing Communication Server* on page 3-5 for the detailed procedure.

Note: You must install the Management Server before the Communication Server.

---

3. Configure Communication Server settings. Refer to *Configuring Communication Server Settings* on page 4-5 for the detailed procedure.
4. Configure SMS senders. Refer to *Installing SMS Sender* on page 3-6 for the detailed procedure.

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

1. Upgrade MSMM to the Management Server for 8.0 SP1:
   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 8.0 SP1 Management 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 Communication Server. Refer to *Installing Communication Server* on page 3-5 for the detailed procedure.

Note: You must install the Management Server before the Communication Server.

4. Configure Communication Server settings. Refer to *Configuring Communication Server Settings* on page 4-5 for the detailed procedure.
5. Configure SMS senders. Refer to *Installing SMS Sender* on page 3-6 for the detailed procedure.

Removing Server Components

This section guides you through the steps you need to perform to remove the Management Server and the Communication Server.

Removing Management Server

Mobile Security Management Server can be removed either automatically or manually:

Removing Management Server Automatically

To remove Management Server automatically:

1. Log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.
3. Click **Uninstall** to remove Management Server. The progress bar displays on the screen showing the uninstallation progress.

Removing Management Server Manually

Although an automatic uninstall is recommended, but if you encounter any problem during automatic uninstall, you can remove the Management Server manually.

To remove Management Server manually:

WARNING! **This procedure requires you to modify registry keys. Making incorrect changes to the registry can cause serious system problems. Always make a backup copy before making any registry changes. For more information, refer to the Registry Editor Help.**

---

1. Delete the related folder in Registry.
   a. Open the Registry Editor, and go to the following key:
   `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS`
   b. Delete folder **OSCE_ADDON_TMMS**
2. Stop the following Windows Services:
   - **OfficeScan Plug-in Manager**
   - **Mobile Security Management Module Service**
   - **Mobile Security Monitor Service**
   - **Mobile Security Management Module BlackBerry Service**
3. On your harddisk, go to **..\Trend Micro\OfficeScan\Addon**, and delete the folder **Mobile Security**.
4. Using the Windows Command Prompt, delete the Mobile Security related services using the following commands:
   - **sc delete TMMSMasterService**
   - **sc delete TMMSMonitorService**
   - **sc delete BBMDMService**
5. On your harddisk:
   - go to **..\Trend Micro\OfficeScan\PCCSRV**, and delete the file ***OSCE_AOS_COMP_LIST.xml***.
   - go to **..\Trend Micro\OfficeScan\PCCSRV\TEMP**, and delete the folder **AoS**

- go to **..\Trend Micro\OfficeScan\PCCSRV\Download**, and delete the following files:
  - ***OSCE_PLS_TMMS.zip***
  - ***OSCE_PLS_TMMS_Install.zip***
  - ***server.ini***

6. Modify the Registry key:
   a. Open the Registry Editor, and go to the following key:
   `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service\AoS`
   b. Modify the **OSCE_Addon_Service_CompList_Version** to **1.0.1000**
7. Start the **OfficeScan Plug-in Manager** service in the Windows Services.

Removing Communication Server

Mobile Security Communication Server can be directly removed from the Windows Control Panel.

To uninstall the Communication Server:

1. From the Windows Control Panel, double-click **Programs and Features**. The **Uninstall or change a program** window displays.
2. Select **Trend Micro Mobile Security Communication Server** and then click **Uninstall**. A dialog box displays.
3. On the dialog box, select **Automatically close applications and attempt to restart them after setup is complete** and click **OK.**
4. Follow the on-screen instructions to complete the uninstallation process.

Chapter 4

Configuring Server Component

This chapter assists administrators in configuring the server components for Trend Micro Mobile Security for Enterprise 8.0 SP1.

This chapter contains the following sections:

Initial Server Setup

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

Initial server setup steps include:

1. *Configuring Database Settings* on page 4-2
2. *Configuring Database Settings* on page 4-2
3. *Configuring Active Directory (AD) Settings* on page 4-4
4. *Configuring Common Communication Server Settings* on page 4-5
5. Installing Certificate Authority (CA) and Simple Certificate Enrollment Protocol (SCEP) server. Refer to *iOS Support Prerequisite* on page 2-3.
6. *Managing Apple Push Notification Service Certificate* on page 4-11
7. *Configuring iOS Communication Server Settings* on page 4-8
8. *Configuring BlackBerry Communication Server Settings* on page 4-10
9. *Managing Apple Push Notification Service Certificate* on page 4-11
10. *Configuring Active Directory (AD) Settings* on page 4-4
11. *Configuring Notifications/Reports Settings* on page 4-12
12. *Configuring Administrator Notifications* on page 4-13

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

Configuring Database Settings

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 user name, password and the database name.

Note: If you are using a specific port for SQL server, use the format:

- For SQL Server: **<SQL server name or IP address>,<Port>**;
- For SQL Server Express: **<SQL server name or IP address>,<Port>\<Instance name of SQL Server Express>**

5. Click **Save**.

Configuring Device Authentication Settings

To configure Device Authentication Settings:

1. Log on to the OfficeScan Web console and click **Plug-in Manager**.
2. Click **Manage Program**.
3. Click **Administration > Device Enrollment Settings**.
4. On the **Authentication** tab, configure the following:
   - **User Authentication**—select one of the following:
     - **Do not authenticate**—to disable user authentication for mobile devices. If you select this setting, then the users do not necessarily need to type their user name and password for registering the mobile devices with the Communication Server.
     - **Authenticate using**—if you select this setting, you can select one or both of the following authentication methods:
       - **Active Directory**—to use the user information from Active Directory to authenticate mobile devices.
       - **Preset user name and password**—to use the user information from the local database to authenticate mobile devices.

Note: If you select **Preset user name and password** for device authentication, you must also type the preset account user name and password in the fields provided.

- **Device Authentication**—select one of the following:
  - **Do not authenticate**—to disable device authentication for mobile devices.
  - **Authenticate using IMEI or Wi-Fi MAC address**—this setting enables you to upload a list of mobile devices that you want to authenticate.
    i. Click **Export allowed device list template** to download the template and create the allowed device list.
    ii. After you have created the list, click **Browse** to select and import the list of mobile devices that you created in the previous step.
    iii. Click **Check Data Format** to verify the data format in the allowed devices list. After verification, Mobile Security displays all the mobile devices in the **Allowed Devices' Status** list.
    iv. Select one of the following options:
      - **Delete unauthenticated devices**—to delete the mobile devices that already exist in the **Device Management** screen but do not exist in the allowed device list that you import.
      - **Display unauthenticated devices in group "Unauthenticated"**—to move all the registered mobile devices that already exist in the **Device Management** screen but do not exist in the allowed device list that you import to the group **Unauthenticated**.

Note: If you use Device Authentication, Mobile Security will regroup all the mobile devices according to the allowed device list that you use.

5. Click **Save**.

Configuring Active Directory (AD) Settings

Trend Micro Mobile Security 8.0 provides you the option to configure user authentication based on the Active Directory (AD). Once configured, you can also use your corporate active directory to add mobile devices to the device list.

If you do not want to use active directory for user authentication or if you do not want to add users from the active directory, then you do not need to configure this setting.

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 user name and your password.
5. Click **Save**.

Configuring Communication Server Settings

Mobile Security 8.0 SP1 provides the following two types of settings for Communication Server:

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

Configuring Common Communication Server Settings

To configure Common Communication Server Settings:

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

   Consider the following while configuring Common Communication Server Settings:

   - **Settings for Communication Between Communication Server and Mobile Devices**:

- If you do not select **HTTPS port** in **Settings for Communication Between Communication Server and Mobile Devices**, the mobile devices will use HTTP port to communicate with the Communication Server.
- iOS 5.x mobile devices support HTTPS only. Therefore, if you want to manage iOS 5.x mobile devices, select HTTPS port to communicate with the Communication Server, and upload the SSL certificate to Mobile Security.

  To upload the SSL certificate to Mobile Security:

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

  ii. Click **Add**, select the certificate, and then click **Save**.
- For basic security model (single server installation), the default ports of Communication Server and Management Server are as follows:
  - HTTP port: 8080
  - HTTPS port: 4343
- For enhanced security model (dual server installation), the default ports of Communication Server are as follows:
  - HTTP port: 80
  - HTTPS port: 443

- **Settings for Communication Between Communication Server and Management Server**:
  - Use the default port number **8189** for SOAP connection. If you need to customize this port number, refer to *Configuring Communication Server Ports* on page B-3 for details.

Note: Mobile Security will collect the information about the applications installed on mobile devices according to the frequency you have selected:

- For iOS mobile devices, Mobile Security will collect this information at the time when iOS mobile device was enrolled.
- For Android mobile devices, Mobile Security will collect this information for the first time when Android mobile device was enrolled, and subsequently at any time between 9:00 AM and 6:00 PM.

Changing the frequency will reset the timer, but Mobile Security will collect this information at the same time of the day.

6. Click **Save**.

Configuring Android Communication Server Settings

To configure Android Communication Server Settings:

1. Log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.
3. Click **Administration** > **Communication Server Settings**.
4. On the **Android Settings** tab, configure the following:
   - **Push Notification Settings**
     - Select **Enable push notification** to enable this setting for Android devices. Clear to disable.
   - **Agent Customization**
     - Select **Enable agent customization** to add the server IP address and port number in the Android client application that users will download from the Mobile Security server. This means, the server IP address and port number will be automatically filled in the client application and users will not need to type this information manually.

       Clear **Enable agent customization** to disable the feature for Android mobile devices.
5. Click **Save**.

Configuring DNS Server for Simpler Android Provisioning

You can configure your DNS Server for simpler provisioning of Android mobile devices by specifying the server information (IP address, domain name and server port number) for the users in advance. By doing this, the server IP address and port number will be automatically filled in the client applications using the users' email addresses only and they will not need to type this information manually.

To configure DNS Server for simpler provisioning of Android mobile devices:

1. Open the **DNS** server console from the Windows Control Panel.
2. Right-click on the domain associated with Mobile Security where you want to add the registration information for the users, and then click **Other New Records**.
3. In the **Select a resource record type** list, select **Text (TXT)**, and then click **Create Record**. The **New Resource Record** window appears.
4. On the **New Resource Record** window, fill the following fields:
   - **Record name**: type the record name. You can leave this field blank if you want to use the parent domain name.
   - **Text**: type the Communication Server address as follows:

     `TM_MDM_SERVER={http://<Communication Server IP>:<Communication Server Port>}`.

     Note: Replace **<Communication Server>** and **<Communication Server Port>** with the original Communication Server IP address and port number.
5. Click **OK**, on the **New Resource Record** window, and then click **Done** on the **Resource Record Type** window.

Configuring iOS Communication Server Settings

To configure iOS Communication Server Settings:

1. Log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.
3. Click **Administration** > **Communication Server Settings**.

4. On the **iOS Settings** tab, configure the following:
   - Simple Certificate Enrollment Protocol (SCEP) Settings
     i. Select **Enable SCEP**. Clear to disable.
     ii. If enabled, fill the fields with the following information:
       - **SCEP user URL:**

         http://SCEP_IP/certsrv/mscep
       - **SCEP admin URL:**

         For Windows Server 2008:

         http://SCEP_IP/certsrv/mscep_admin

         For Windows Server 2003:

         http://SCEP_IP/certsrv/mscep
       - **User account:** <SCEP Server login user name>
       - **User password:** <SCEP Server login user 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 drop-down list, or upload a new one.
   - Client Profile Signing Credential
     - **Client Profile Signing Credential:** Select a certificate for signing credential from the drop-down list, or upload a new one.
5. Click **Save**.

Configuring BlackBerry Communication Server Settings

Note: Before configuring BlackBerry Communication Server settings, you must install **brk-besuseradminclient** command tool on the Mobile Security Management 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 Communication Server Settings:

1. Log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.
3. Click **Administration** > **Communication Server Settings**.
4. On the **BlackBerry Settings** tab, fill all the fields with the following information.
   - **BlackBerry Administration Service Credentials**
     - **Server name**:<BES server name (your computer name) or IP address where you have installed the BES Administration Service>
     - **User account**: <administrator name for the BES Administration Service>
     - **Password**: <password for the user account>
     - **Domain name**: <BES server domain name>

     Note: If your OfficeScan server cannot connect with BES server using BES server name, type the BES server IP address in the **Server name** field.

   - **BlackBerry Database Settings**
     - **Database address**: <BES configuration database name or IP address>
     - **User name**: <database user name>

     Note: You need to create a database user with the Connection and Read permissions for the database.

- **Password**: <Database user login password>
- **Database name**: <BES configuration database name>

Note: For BlackBerry Database settings, Trend Micro Mobile Security only supports **SQL Server** authentication mode for SQL server.

- **BlackBerry Command Tool Settings**
  - **Tool path**: <BlackBerry Administration Tool installation path. For example: `C:\Program Files\Research In Motion\BlackBerry Enterprise Server Resource Kit\BlackBerry Enterprise Server User Administration Tool Client>`

5. Click **Save**.

Managing Apple Push Notification Service Certificate

Refer to *Generating and Configuring APNs Certificate* starting on page C-1 for the detailed procedure of generating the APNs certificate and then uploading it to the Mobile Security server.

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**.

Using Configuration and Verification

This screen enables you to quickly configure Mobile Security settings. It also enables you to verify if all the settings that you have configured are correct.

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** > **Configuration and Verification**.
4. You can now configure and verify Mobile Security settings:
   - To configure Mobile Security settings, read instructions on the screen and click on the text to open the settings screen.
   - To verify Mobile Security settings, click **Verify Mobile Security Configuration**.

Configuring Notifications/Reports Settings

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

To configure Notifications/Reports Settings:

1. Log on to the OfficeScan Web console and click **Plug-in Manager**.
2. Click **Manage Program**.
3. Click **Notifications/Reports > 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 user name 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 Communication 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** Communication Server**.**

Configuring Administrator Notifications

You can configure Administrator Notifications and Reports setting to receive the error message notifications and regular scheduled reports via email.

To configure notifications and reports send to administrator:

1. Log on to the OfficeScan Web console and click **Plug-in Manager**.
2. Click **Manage Program**.
3. Click **Notifications/Reports > Administrator Notifications/Reports**.
4. Select the notifications and reports you want to receive via email, and then click on individual notifications and reports to modify their contents. Click **Save** when done, to return back to the **Administrator Notifications and Reports** screen.

   Note: When you select reports that you want to receive, you can also adjust their frequencies individually from the drop-down list after each report.

5. Click **Save**.

Chapter 5

Handling Mobile Device Agent

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 Communication 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 5-1. 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
iOS 4.x or above	4	3

Note: For Blackberry mobile devices, Mobile Security supports BES 5.x.

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

Mobile Device Agent Installation Methods

For iOS mobile devices, you can install Mobile Device Agent from the Apple store using the following URL:

http://store.apple.com/mobile_security (to be updated)

For Android, Symbian or Windows mobile devices you can install Mobile Device Agent 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 Communication Server. You need to install the SMS senders if you want to send SMS notification messages.
- Installation through Web browser—in the Web browser, open the following URL to automatically download and install the Mobile Device Agent on mobile devices:

  http://<External_domain_name_or_IP_address:HTTP_port>/mobile

  or

  https://<External_domain_name_or_IP_address:HTTPS_port>/mobile

  Note: Replace **<External_domain_name_or_IP_address>**, **<HTTP_port>** and **<HPTTS_port>** as you configured in **Administration** > **Communication Server Settings** > **Common Settings** > **Settings for Communication Between Communication Server and Mobile Devices**.

  If you need to customize the enrollment URL, refer to *Customizing Enrollment URL for Mobile Devices* on page 5-4 for the details.

- Memory card—for Symbian or Windows platforms, download the setup file from the Management 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 8.0 SP1 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 Communication Server. For detailed instructions on manual installation and registration, refer to *Launching the Setup File Manually* on page 5-9 or the User's Guide for your mobile device platform.

Customizing Enrollment URL for Mobile Devices

To enroll a Mobile Device Agents to the Communication Server through the Web, the Mobile Device Agents must access the following URL:

http://<External_domain_name_or_IP_address:HTTP_port>/mobile

or

https://<External_domain_name_or_IP_address:HTTPS_port>/mobile

To customize the enrollment URL for mobile devices:

1. Modify the enrollment URL:
   a. On the Management Server, go to the folder **`..\Trend Micro\OfficeScan\Addon\Mobile Security`**, and Security.
   b. Open the file `TmOMSM.ini` in a text editor.
   c. Modify the value of `tmms_provision_shortlink_preset` as per your requirement.

   Note: Make sure that there is not virtual directory with the name that you choose in `tmms_provision_shortlink_preset`.

2. Update the enrollment URL in the **Communication Server**:
   a. Log on to the OfficeScan Web console and click **Plug-in Manager**.
   b. Click **Manage Program** for Mobile Security.
   c. Click **Administration** > **Communication Server Settings**.
   d. Click **Save**.

3. If you do not want to use the old enrollment URL, then delete the old enrollment URL from the Internet Information Services (IIS) Manager:
   a. Start Internet Information Services (IIS) Manager.
   b. From the **Connection** tree on the left side of the screen, right-click **TMMS** > **Sites** > **OfficeScan** > [the enrollment URL name you want to delete], and then click **Remove**.
   c. Close Internet Information Services (IIS) Manager.

Installing Mobile Device Agent

To use the encryption and password 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 and password 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 Notifications/Reports Settings* on page 4-12
- *Configuring Installation Message* on page 5-5
- *Configuring the Mobile Device List* on page 5-6

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 email or 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 **Notifications/Reports > User Notifications**.
4. Select **Mobile Device Enrollment**, and then click on the text.
5. Type the subject, email and/or the text message in the related text box(es), and then click **Save**.

Note: The installation message must include the characters "%DOWNLOADURL%" 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.

6. Click **Save** on the User Notifications screen.

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, the Mobile Security server will automatically add Mobile Device Agent information to the list after the device is registered to the Mobile Security Server.

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 **Devices**. The Device Management screen displays.
4. You can now add one mobile device, a batch of mobile devices, a user or an email group (distribution list) from the active directory:
   - To add a mobile device:
     i. Click **Add Device** > **Add Device**. The **Add Device** window pops up.
     ii. On the **Add Device** window, configure the following fields:
     - **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.
     - **Group**—select the name of the group to which the mobile device belongs from the drop-down list. You can always change the group to which the mobile device agent belongs.

     Tip: To add more devices, click the [+] button.

   - To add a batch of mobile devices:
     i. Click **Add Device** > **Add Batch**.
     ii. Type the device information in the text box on the window that displays.
     iii. Click **Validate** to verify that the device information conforms to the specified format.
   - To add a user or an email group (distribution list) from the active directory:
     i. Click **Add Device** > **Add from AD**.
     ii. Type the user information in the field provided, and click **Search**.
     iii. Select the user from the search result, and then click **Add to Device List**.

5. Click **Save**.
6. 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 Dashboard screen for Mobile Security in the 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 Enrollment Settings**.
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 server. Select an AP that your mobile device use to connect to the Communication 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 mobile devices, you can use PC Sync to install Mobile Device Agent directly from the host computer.

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 Enrollment Settings**.
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, users can be instructed to download and install the mobile device agent by visiting the following URL:

   http://<External_domain_name_or_IP_address:HTTP_port>/mobile

   or

   https://<External_domain_name_or_IP_address:HTTPS_port>/mobile

   Note: Replace **<External_domain_name_or_IP_address>**, **<HTTP_port>** and **<HPTTS_port>** as you configured in **Administration** > **Communication Server Settings** > **Common Settings** > **Settings for Communication Between Communication Server and Mobile Devices**.

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 Mobile 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 Communication 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. Start the Mobile Device Agent program on the mobile device.
2. The **Register** screen displays. Do one of the following:
   - On Symbian and Windows Mobile devices: Type a descriptive name for the device, the DNS name or IP address, HTTP or HTTPS port number of the Communication Server, your domain user name and its password. Click **Register**.

     Note: Symbian mobile devices can only use HTTP to communicate with the Communication Server. Windows Mobile devices can only use HTTP to register, but can use HTTP or HTTPS for further communications depending on the settings you configured in **Settings for Communication Between Communication Server and Mobile Devices** while configuring the common Communication Server settings. See *Configuring Common Communication Server Settings* on page 4-5.

   - On Android mobile devices: type your email address and tap **Next**. Type your domain user name and password, and then tap **Register**.
3. After the registration is completed, view the license information in the About screen (**Menu** > **About**) on the mobile device. You can also see the device status on the Mobile Security server.

Note: The registration process may take several minutes depending on your network speed.

iOS Provisioning

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

WARNING! **The JavaScript must be enabled for Safari on iOS mobile devices for enrollment. Otherwise, the enrollment will be unsuccessful.**

To install the provisioning profile on an iOS mobile device:

1. On the iOS mobile device, do one of the following:
   - Open the Mobile Device Agent program, then on the **Enroll to Mobile Security Server** screen, type your email address, and then tap **Enroll this Device**.

     Note: If you want to use the Server IP address and Port number to enroll your mobile device, tap **Manual Setup** on the **Enroll to Mobile Security Server** screen. Then, type the Server IP address and Port number, and then tap **Enroll this Device**.

     The **Install Profile** screen displays.
   - Open the Safari Web browser, and go to the following URL:

     http://<External_domain_name_or_IP_address:HTTP_port>/mobile

     or

     https://<External_domain_name_or_IP_address:HTTPS_port>/mobile

     Note: Replace **<External_domain_name_or_IP_address>**, **<HTTP_port>** and **<HPTTS_port>** as you configured in **Administration** > **Communication Server Settings** > **Common Settings** > **Settings for Communication Between Communication Server and Mobile Devices**.

     Note: If the authentication is required by the administrator, the **Authentication Required** pop-up dialog box appears. Type your domain account (or user name) and password, and then tap **Log In**.

     The **Install Profile** screen displays.

2. On the **Install Profile** screen, tap **Install**, and then tap **Install Now** on the confirmation pop-up dialog box.
3. 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.
4. Tap **Install** on the **Warning** confirmation screen. The profile installation process begins. After the process is completed, the **Profile Installed** screen displays.
5. Tap **Done**.

To uninstall the provisioning profile from an 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.

Note: For iOS 5.x mobile device, removing the profile will move the mobile device to the group **"Unmanaged"** on the Mobile Security server.

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 module supports the mobile device platform

Note: The encryption in Mobile Security for Enterprise 8.0 SP1 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 (only for Windows Mobile devices):

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 5-12.
2. encryption and passwordAfter registration, you are prompted to provide an initial power-on password to log on the device. By default, the initial password is **123456**.

Appendix A

Firewall Ports Configurations

This appendix provides all the firewall ports configurations that you need while installing Trend Micro Mobile Security, and brings together all the firewall ports configurations mentioned in the document.

This appendix contains the following sections:

Firewall Ports Configuration for Basic Security Model (Single Server Installation)

If you are using the basic security model, configure the following firewall ports for Mobile Security components:

COMPONENT	FIREWALL PORTS	DETAILS
Management Server and Communication Server	Open TCP port **2195** for Apple Push Notification service (APNs) server. The hostname of Apple Push Notification Service is **`gateway.push.apple.com`**.	Enables Apple's APNs server to manage iOS mobile devices. If you are not managing iOS mobile devices, this port is not required.
	Open HTTP port **8080**. **Note:** This is the default HTTP port number for the singe server configuration. However, you can change the HTTP port number that you want to use for mobile devices to communicate with the Mobile Security server during the installation.	Used for communication between mobile devices and the Mobile Security server.
	Open HTTPS port **4343**. **Note:** This is the default HTTPS port number for the singe server configuration. However, you can change the HTTPS port number that you want to use for mobile devices to communicate with the Mobile Security server during the installation.	Used for secure communication between mobile devices and the Mobile Security Server.

COMPONENT	FIREWALL PORTS	DETAILS
Active Directory	Open one of the following ports: • TCP port **389** (Domain Controller) for Management Server and Communication Server • TCP port **3268** (Global Category) for Management Server and Communication Server	Used for user authentication using Active Directory. If you are not using Active Directory to authenticate or import users, this port is not required.
Simple Certificate Enrollment Protocol (SCEP) Server	Open HTTP port **80** for Communication Server and iOS mobile devices.	Used for iOS mobile devices enrollment. If you are not using SCEP server to manage iOS mobile devices, this port is not required.
SQL Server	Open the following ports: • TCP port **1433** for Mobile Security server. • UDP port **1434** for Mobile Security server. **Note:** This is the default TCP port to connect to the SQL Server. However, you can also use a different port for SQL server, if required.	Establishes a connection between the Mobile Security server and the remote SQL server.
BlackBerry Enterprise Server (BES)	Open the following ports: • Open TCP port **3101** for BES Server Routing Protocol (SRP) Infrastructure. • Open TCP port **443** for Management Server and BES command tool	If you are not using Mobile Security to manage BlackBerry mobile devices, these port are not required.

Firewall Ports Configuration for Enhanced Security Model (Dual Server Installation)

If you are using the enhanced security model, configure the following firewall ports for Mobile Security components:

COMPONENT	FIREWALL PORTS	DETAILS
Communication Server	Open the following port for Apple Push Notification service (APNs) server: • TCP port **2195**: gateway.push.apple.com	Enables Apple's APNs server to manage iOS mobile devices. If you are not using APNs server to manage iOS mobile devices, this port is not required.
	Open HTTP port **80.** **Note:** This is the default HTTP port number for the dual server configuration. However, you can change the HTTP port number that you want to use for mobile devices to communicate with the Communication Server during the installation.	Used for communication between mobile devices and the Communication Server.
	Open HTTPS port **443**. **Note:** This is the default HTTPS port number for the dual server configuration. However, you can change the HTTPS port number that you want to use for mobile devices to communicate with the Communication Server during the installation.	Used for secure communication between mobile devices and the Communication Server.

COMPONENT	FIREWALL PORTS	DETAILS
Communication Server	Open the following ports: • TCP port **8189**: the default port for Simple Object Access Protocol (SOAP) connection to allow inbound connection to Communication Server from Management Server • TCP port **8190**: the default port for socket connection to allow inbound connection to Communication Server from Management Server	Establishes a connection between the Management Server and the Communication Server.
Active Directory	Open one of the following ports: • TCP port **389** (Domain Controller) for Management Server and Communication Server • TCP port **3268** (Global Category) for Management Server and Communication Server	Used for user authentication using Active Directory. If you are not using Active Directory to authenticate or import users, this port is not required.
Simple Certificate Enrollment Protocol (SCEP) Server	Open HTTP port **80** for Communication Server and iOS mobile devices.	Used for iOS mobile devices enrollment. If you are not using SCEP server to manage iOS mobile devices, this port is not required.

COMPONENT	FIREWALL PORTS	DETAILS
SQL Server	Open the following ports: • TCP port **1433** for Communication Server and Management Server • UDP port **1434** for Communication Server and Management Server. **Note:** TCP port **1433** is the default port to connect to the SQL Server. However, you can also use a different TCP port for SQL server, if required.	Establishes a connection between the Communication Server and the Management Server with the remote SQL server.
BlackBerry Enterprise Server (BES)	Open the following ports: • Open TCP port **3101** for BES Server Routing Protocol (SRP) Infrastructure. • Open TCP port **443** for Management Server and BES command tool	If you are not using Mobile Security to manage BlackBerry mobile devices, these port are not required.

Appendix B

Optional Configurations

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

This appendix contains the following sections:

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. Create a domain account in Active Directory server with the rights to access Mobile Security database.
2. Add the Management Server and the Communication Server to the domain you created in step 1.
3. On the Management Server, open Windows Services, and double-click **OfficeScan Plug-in Manager.**
4. 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**.
5. Right-click on the **OfficeScan Plug-in Manager** in the services list, and then click **Restart**.
6. On the Management Server, repeat steps 3 to 5 for the following services:
   - Mobile Security Management Module Service
   - Mobile Security Monitor Service
   - Mobile Security Management Module BlackBerry Service
7. On the Communication Server, repeat steps 3 to 5 for the following service:
   - Mobile Security Management Module IOS Service
   - Mobile Security Communication Module (MSCM) server
8. 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 database server IP address and the database name, and leave the **User name** and **Password** fields blank.
   e. Click **Save**.

Configuring Communication Server Ports

Trend Micro Mobile Security 8.0 SP1 enables to you to customize the Communication Server ports that it uses to establish the connection with the Management Server.

To configure Communication Server ports:

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

      or

      `C:\Program Files(x86)\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 `TmOMSM.ini` file.
   d. Open Windows services, and right-click **OfficeScan Master Service**, and then click **Restart**.
2. Configure socket and SOAP ports on the Communication Server:
   a. On the Communication 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 Management 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 do the following:
   - 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

Appendix C

Generating and Configuring APNs Certificate

Trend Micro Mobile Security requires the Apple Push Notification service (APNs) certificate to manage iOS mobile devices. This appendix introduces the detailed procedure of generating the APNs certificate and then uploading it to the Mobile Security server.

This appendix contains the following sections:

Understanding APNs Certificate

The Apple Push Notification service (APNs) enables Trend Micro Mobile Security for Enterprise server to securely communicate to your devices over-the-air (OTA). Each organization needs its own APNs certificate to ensure a secure mechanism for their devices to communicate across Apple's push notification network.

Trend Micro Mobile Security for Enterprise uses your APNs certificate to send notifications to your devices when the Administrator requests information or manage your iOS devices. Only the notification is sent through the APNs server.

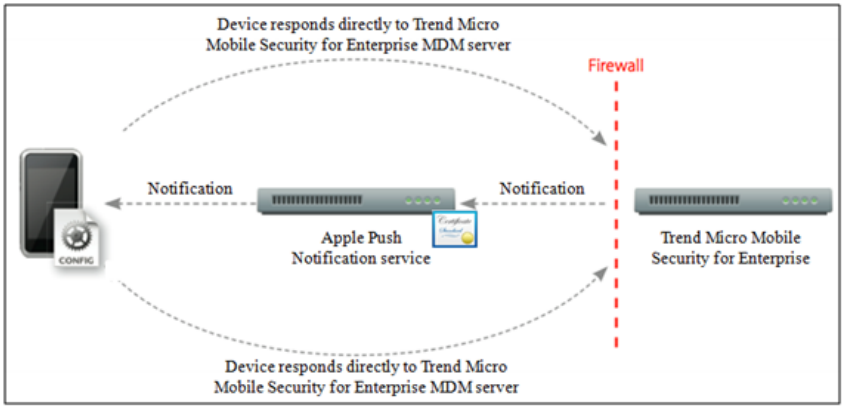

FIGURE C-1. Notification process

Generating an APNs Certificate

This section explains the process of generating Apple Push Notification Service certificate for iOS mobile devices management.

The following are the basic steps for Generating APNs certificate:

1. Generate a Certificate Signing Request (CSR).
2. Do one of the following:
   - Use the certificate signed by Trend Micro
     i. Send the generated CSR to Trend Micro. Trend Micro will sign and return you the CSR.
     ii. Upload the CSR to Apple Push Certificates Portal.
   - Use the certificate signed by Apple
     - Upload the CSR to your Apple Development portal. (Apple will sign your certificate.)
3. Download the signed certificate from the Apple portal and complete the initial CSR request.

Note: Make sure that you have the following before you begin:

- To use the certificate signed by Ternd Micro:
  - Apple ID
- To use the certificate signed by Apple:
  - Apple Enterprise Developer account (developer.apple.com/programs/ios/enterprise)
  - Your developer account role must be Agent (Admin role will not work)
  - Mac OS X workstation or Windows Server with Administrator permissions

---

Generating an APNs Certificate from a Mac Workstation

The following procedure will guide you to generate an APNs certificate using a Mac OS X workstation. For Windows Server you may skip this section, and proceed to *Generating an APNs Certificate from a Windows Server* on page C-8.

Step 1. Generate a Certificate Signing Request (CSR)

1. On you Mac computer, go to **Applications** > **Utilities** > **Keychain Access**.
2. On the left pane, select login in the **Keychain** section, and then select **Certificates** in the **Category** section.
3. From the top menu bar, select **Keychain Access** > **Certificate Assistant** > **Request a Certificate From a Certificate Authority**. The **Certificate Assistant** wizard displays.
4. Type the email address and registered Apple Developer account name in **User Email Address** and **Common Name** fields, select **Saved to disk**, and then click **Continue**.
5. Select the location where you want to save the file, and then click **Save**. You have now created a CSR and are ready to upload it to your Apple development portal.

Step 2. Uploading CSR to Apple portal and generating the APNs certificate

After you have generated the CSR, you can now do one of the following:

- Send the CSR you have just generated to Trend Micro to sign it for you, and then use it to generate APNs certificate.
- Upload the CSR to Apple development portal to get it signed by Apple, and then use it to generate APNs certificate.

To use the certificate signed by Trend Micro

1. Send the CSR you have just generated to your Trend Micro representative. Trend Micro will sign it and return it to you.
2. After you have received the signed CSR back from Trend Micro, upload the CSR to Apple Push Certificates Portal:
   a. Open the Web browser and navigate to the following URL:
   https://identity.apple.com/pushcert/.
   b. Sign in with your Apple ID and password. The **Get Started** page displays.

c. Click **Create a Certificate** button. The **Terms of Use** screen appears.

d. Click **Accept** to agree with the terms. **Create a New Push Certificate** screen displays.

e. Click **Browse**, select the file already signed by Trend Micro, and then click **Upload**. Wait until the portal generates the APNs certificate (**`.pem`**) file.

f. Click **Download** to save the **`.pem`** file to your computer, and then proceed to *Step 3. Install your APNs certificate* on page C-7 for Mac or *Step 3. Install your APNs certificate* on page C-11 for Windows.

To use the certificate signed by Apple

Note: Skip this procedure if you are using the APNs certificate signed by Trend Micro.

1. On the Web browser, navigate to the following URL: https://developer.apple.com/.
2. Click the **Member Center** link.
3. Sign in with your Apple ID and password.
4. Click **iOS Provisioning Portal**.

Note: If you do not see the iOS Provisioning Portal, your development account has not been setup for iOS development.

5. On the left pane, click **App IDs**, and then click **New App ID**.
6. Fill in the applicable fields. T**he Bundle Identifier (App ID Suffix) notation** field must be "`com.apple.mgmt.mycompany.tmms`"

Note: Replace **mycompany** with your company name.

Note: Note down The Bundle Identifier (App ID Suffix) notation value. You will need this value while configuring Mobile Security server.

7. Click **Submit**. The **App ID** that you have just added, appears in the list.

8. Click **Configure**.

   Tip: If you do not see or cannot click **Configure**, verify that you are signed in with the Agent role.

9. Select **Enable for Apple Push Notification service**, and then click **Configure** for Production Push SSL Certificate.

   Tip: If you are unable to select **Enable for Apple Push Notification service**, try using Safari or Firefox Web browser, and verify that you are singed in with the Agent role.

10. **SSL Certificate Assistant** wizard will appear, instructing you to create a Certificate Signing Request (that you have already created in *Step 1. Generate a Certificate Signing Request (CSR)*). Click **Continue**.
11. Click **Choose File** and upload the Certificate Signing Request file that you created in *Step 1. Generate a Certificate Signing Request (CSR)*. (For example, CertificateSigningRequest.certSigningRequest2).
12. Click **Generate**.

    When completed, the screen will appear confirming that your APNs SSL certificate has been generated.
13. Click **Continue**. The **Download & Install Your Apple Push Notification server SSL Certificate** screen displays.
14. Click **Download** to save the `.cer` file to your computer, and then proceed to *Step 3. Install your APNs certificate* on page C-7 for Mac or *Step 3. Install your APNs certificate* on page C-11 for Windows.

    Note: To install the APNs certificate on Windows computer, you must manually change the file extension from `.pem` to `.cer`.

Step 3. Install your APNs certificate

1. Go to the location where you downloaded the file, and then double-click the file to automatically uploaded it to Keychain Access and complete the signing request.
2. Go to **Applications** > **Utilities** > **Keychain Access**.
3. On the left pane, select **login** in the Keychain section, and then select **Certificates** in the Category section.
4. Verify that your Apple Production Push Services certificate appears on the list, and it has an associate private key beneath it when you expand it. If you can see the certificate, follow the next steps to export the certificate and upload it to the Trend Micro Mobile Security server.

Tip: If you do not see your APNs certificate or the private key is not showing, verify you have the login keychain selected, the Certificates category selected and your certificate key has been expanded. If you still do not see your certificate, repeat all of the steps above.

---

5. Right-click (or control+click) on the private key and click **Export**.
6. Choose the file name and location where you want to save the file, and then select **Personal Information Exchange (`.p12`)** file format.

Tip: If you only have the option to save as a **`.cer`** file rather than a **`.p12`**, then you are not correctly exporting the certificate. Make sure you selected the **private key** to export in the last step, and your file format is **Personal Information Exchange (`.p12`)**.

---

7. Click **Save**.
8. Choose a password for exporting, and then click **OK**.

Tip: Make sure to remember the password, or keep it in the secure place. The password will be required when uploading the certificate to Trend Micro Mobile Security for Enterprise MDM server.

After completing all these steps, you should have the following items:

- APNs certificate (`.p12` format, not `.cer` format)
- The password that you set when exporting the certificate

You are now ready to upload your certificate to Trend Micro Mobile Security server.

Generating an APNs Certificate from a Windows Server

The following steps will guide you to generate an APNs certificate from a Windows Server. If you have already generated your certificate from a Mac OS X workstation, you can skip this section and upload your certificate to Trend Micro Mobile Security for Enterprise MDM server.

Step 1. Generate a Certificate Signing Request (CSR)

1. Go to **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**, and select the server name.
2. Double-click **Server Certificates** icon.

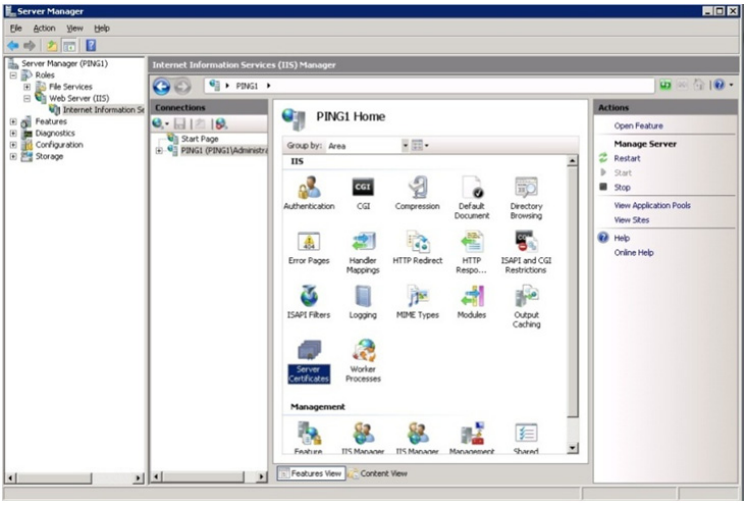

FIGURE C-2. Accessing Server Certificates

Note: The IIS version 7.0 is used to configure APNs certificate in this document.

3. From the Actions pane on the right, click **Create Certificate Request**. The **Request Certificate** wizard appears.

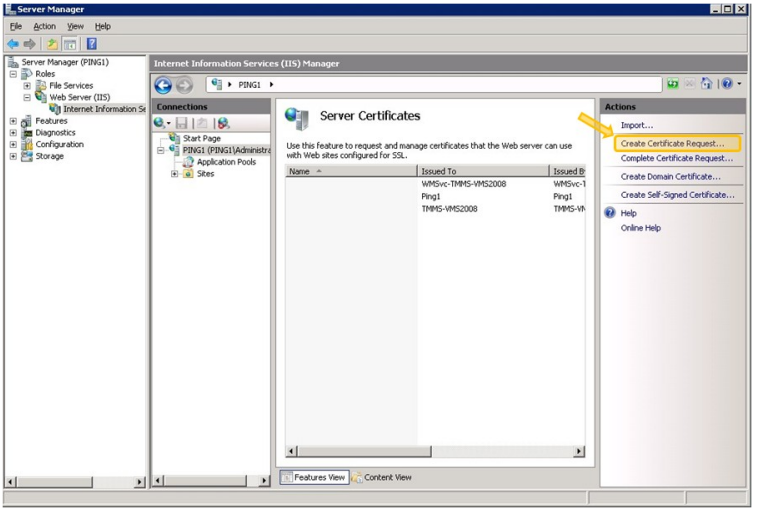

FIGURE C-3. Starting Request Certificate wizard

4. In the **Distinguished Name Properties** window, type the following:
   - **Common name—**the name associated with your Apple Developer account
   - **Organization—**the legally registered name of your organization/company
   - **Organizational unit—**the name of your department within the organization
   - **City/locality—**the city in which your organization is located
   - **State/province—**the state or province in which your organization is located
   - **Country/region—**the country or region in which your organization is located

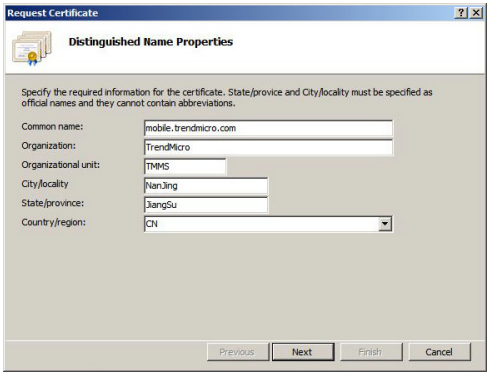

FIGURE C-4. Distinguished Name Properties screen

5. Click **Next**. Cryptographic Service Provider Properties window appears.
6. Select **Microsoft RSA SChannel Cryptographic Provider** in the **Cryptographic service provider** field and **2048** in the **Bit length** field, and then click **Next**.

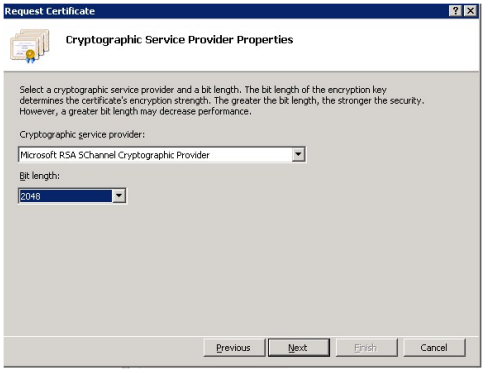

FIGURE C-5. Cryptographic Service Provider Properties screen

7. Select a location where you want to save the certificate request file. Make sure to remember the filename and the location where you save the file.

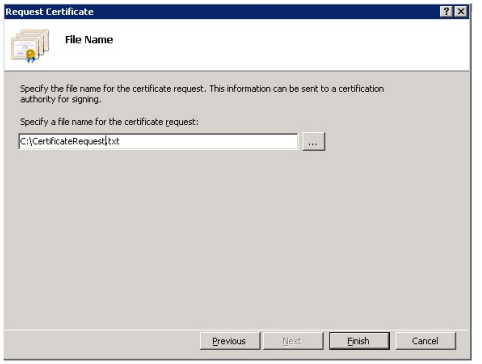

FIGURE C-6. File Name screen

8. Click **Finish**. You have now created a CSR and are ready to upload it to your Apple development portal.

Step 2. Upload CSR to Apple portal and generating the APNs certificate

Refer to *Step 2. Uploading CSR to Apple portal and generating the APNs certificate* on page C-4 for Mac OS X for the procedure.

Step 3. Install your APNs certificate

1. Go to **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**, select the server name, and then double-click **Server Certificates**
2. From the **Actions** pane on the right, click **Complete Certificate Request**. The Complete Certificate Request wizard appears.

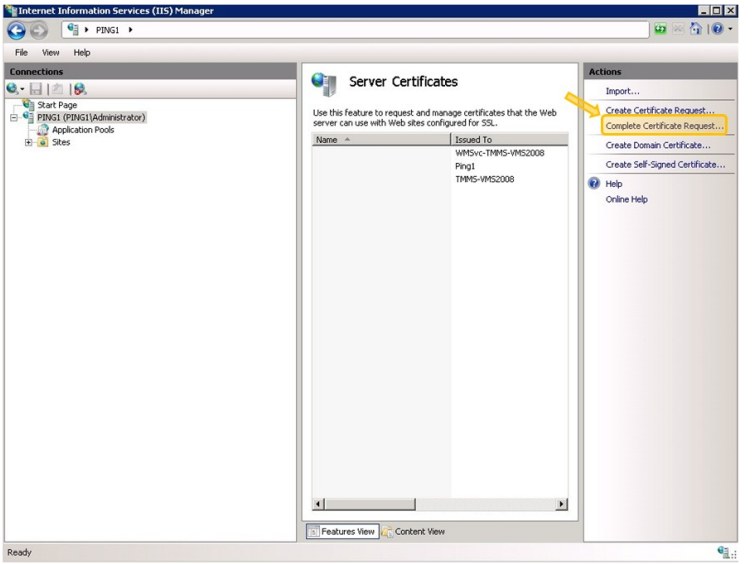

FIGURE C-7. Complete Certificate Request

Note: If you are using IIS 7.5, clicking **Complete Certificate Request** may display the following error message:

A certificate chain could not be built to a trusted root authority.

If this happens, refer to *Configure IIS 7.5 for APNs Certificate Installation on page C-15* for the procedure to resolve this issue.

---

3. Select the **`.cer`** certificate file that you downloaded from the Apple Developer Portal, and type **Trend Micro Mobile Security for Enterprise MDM APNs** in the **Friendly name** field.

Note: If you generated the certificate file from the Mac Workstation, you must manually change the **`.pem`** file extension to **`.cer`**.

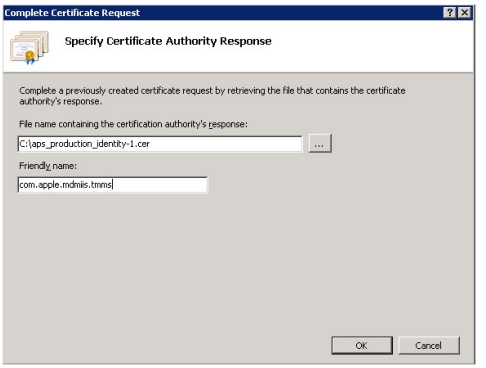

FIGURE C-8. Specify Certificate Authority Response screen

Tip: The friendly name is not a part of the certificate itself, but is used by the server administrator to easily distinguish the certificate.

4. Select **OK**. The certificate will be installed on the server.
5. Verify that your Apple Production Push Services certificate appears on the **Server Certificates** list. If you can see the certificate, follow the next steps to export the certificate and upload it to the Trend Micro Mobile Security for Enterprise MDM server.
6. Right-click on the certificate in the **Server Certificates** list, and then click **Export**.

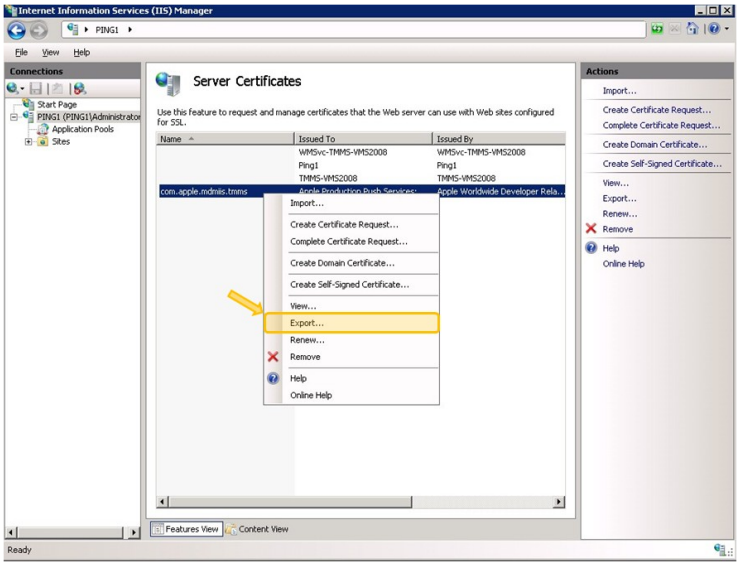

FIGURE C-9. Exporting the certificate

7. Select the location where you want to save the file, choose a password for exporting, and then click **OK**.

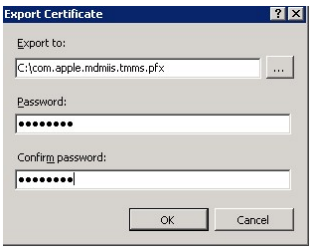

FIGURE C-10. Specifying password for the certificate

Tip: If you only have the option to save as a **`.cer`** file rather than a `.pfx`, then you are not correctly exporting the certificate. Make sure you selected the correct file to export.

Note: Make sure to remember the password, or keep it in the secure place. The password will be required when uploading the certificate to Trend Micro Mobile Security for Enterprise MDM server.

After completing all these steps, you should have the following items:

- APNs certificate (**`.pfx`** format, not **`.cer`** format)
- The password that you set when exporting the certificate

You are now ready to upload your certificate to Trend Micro Mobile Security server.

Configure IIS 7.5 for APNs Certificate Installation

If you are using IIS 7.5, uploading the certificate to IIS may fail with the following message:

A certificate chain could not be built to a trusted root authority.

This can happen due to the following reasons:

- The APNs certificate is signed by the Apple Root CA instead of a public CA.
- The enhanced check for the trusted root CA by IIS 7.5.

To configure IIS 7.5 for APNs certificate installation:

1. Download the **Apple Root** certificate and **Application Integration** certificate from the following URL:

   http://www.apple.com/certificateauthority/

2. Double-click **Apple Root** certificate, and then on the **Certificate** window, click **Install Certificate**.
3. On the welcome screen, click **Next**.
4. Select **Place all certificates in the following store** and then click **Browse**.
5. On the **Select Certificate Store** window, select **Show physical stores**, then select **Trusted Root Certification Authorities** > **Local Computer** and then click **OK**.

6. Click **Next** on the **Certificate Import Wizard** screen, then click **Finish**.
7. Repeat step 2 to 5 for **Application Integration** certificate. However, in step 4, select **Intermediate Certification Authorities** > **Local Computer** instead of **Trusted Root Certification Authorities** > **Local Computer**.

Uploading APNs Certificate to Mobile Security Server

This section explains the process of uploading Apple Push Notification service (APNs) certificate to Trend Micro Mobile Security for Enterprise server to start managing iOS devices.

Note: Make sure that you have the following before you begin:

- APNs certificate file (the `.pfx` or `.p12` format, not the `.cer` format)
- The password that you had set when exporting the certificate
- The administrator account of Trend Micro Mobile Security for Enterprise MDM server

---

To upload APNs certificate to Mobile Security:

1. Open Internet Explorer, and log on to the OfficeScan Web console.
2. Click **Plug-in Manager** in the main menu.
3. Do one of the following:
   - Click **Administration** > **Certificate Management**, click **Add**, select the Apple Push Notification Server certificate from the hard disk, and then click **Save**.

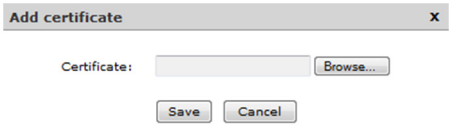

FIGURE C-11. Add certificate through Certificate Management

- Click **Administration** > **Communication Server Settings**, click **iOS Settings** tab, and then select the Apple Push Notification Server certificate from the hard disk in the **Certificate** field, and then click **Save**.

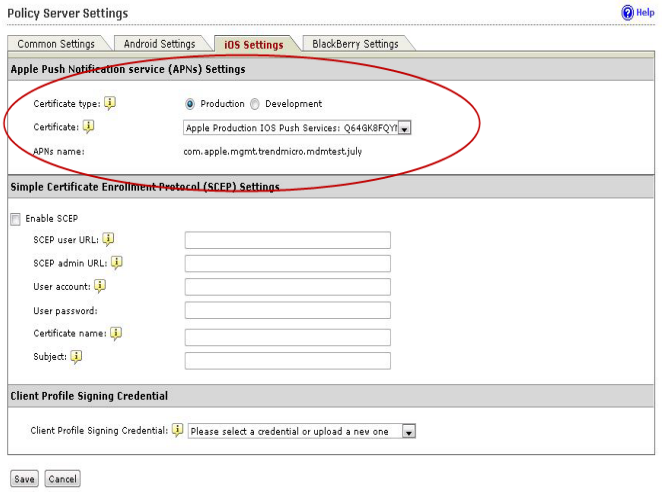

FIGURE C-12. Add certificate through Communication Server settings

After completing these steps, you can now manage your iOS mobile devices.

Generating and Configuring APNs Certificate in Windows 2003 Server Using IIS 6.0

Refer to the following URL for the detailed steps on generating and configuring APNs certificate in Windows 2003 Server using Internet Information Services (IIS) 6.0:

http://esupport.trendmicro.com/solution/en-us/1060668.aspx

Appendix D

Generating and Configuring SSL Certificate

Trend Micro Mobile Security requires a private Secure Socket Layer (SSL) server certificate issued from a recognized Public Certificate Authority for the secure communication between mobile devices and Communication Server using Secure Hypertext Transfer Protocol (HTTPS). This appendix introduces the detailed procedures of generating a private SSL certificate and obtaining a public SSL certificate from a recognized Public Certificate Authority, and then deploying the to Internet Information Services (IIS) Manager on the Communication Server.

This appendix contains the following sections:

Generating and Installing a Private SSL Certificate on Communication Server

This section explains the process of generating a private SSL certificate for HTTPS for iOS mobile devices.

The following are the basic steps for generating and installing a private SSL certificate:

1. Install a standalone Certification Authority (CA) on the Communication Server.
2. Generate a Certificate Signing Request (CSR) for the SSL certificate.
3. Sign and export the SSL certificate.
4. Complete the initial CSR request.
5. Install SSL certificate on iOS mobile devices.

Step 1. Install a standalone Certification Authority (CA) on the Communication Server

1. Go to **Start** > **Administrative Tools** > **Server Manager**
2. On the **Server Manager** tree in the left pane, click **Roles**, and then in the **Roles Summary** section, click **Add Roles**. The **Add Roles Wizard** displays.

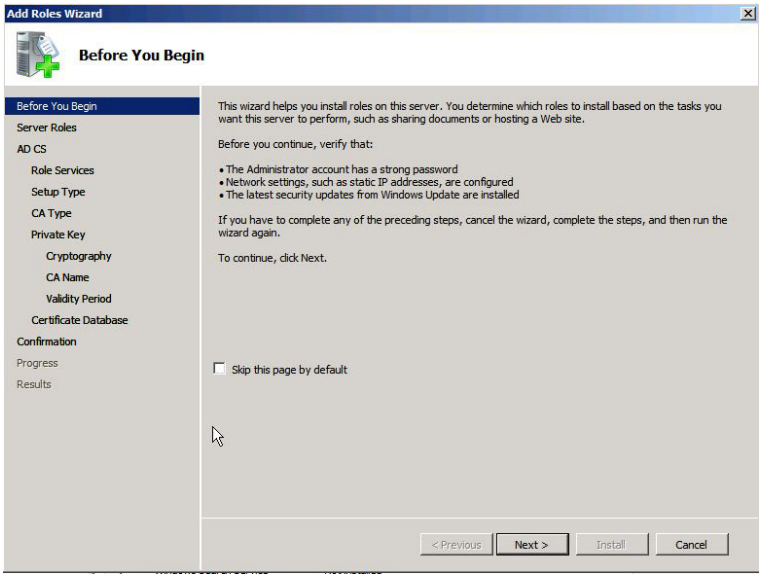

FIGURE D-13. Add Roles Wizard window

3. On the **Before You Begin** screen, click **Next**.
4. From the **Roles** list, select **Active Directory Certificate Services**, and click **Next**.
5. On the **Introduction to Active Directory Certificate Services** screen, click **Next**.
6. In the **Role services** list, select **Certification Authority**, and click **Next**.
7. On the **Specify Setup Type** screen, select **Standalone** and click **Next**.
8. On the **Specify CA Type** screen, select **Root CA** and click **Next**.
9. On the **Set Up Private Key**, select **Create a new private key** and click **Next**.
10. On the **Configure Cryptography for CA** screen, configure the fields as follows:
    - **Select a cryptographic service provider (CSP)**: `RSA#Microsoft Software Key Storage Provider`
    - **Key character length**: `2048`
    - **Select the hash algorithm for signing certificates issued by this CA**: `sha1`

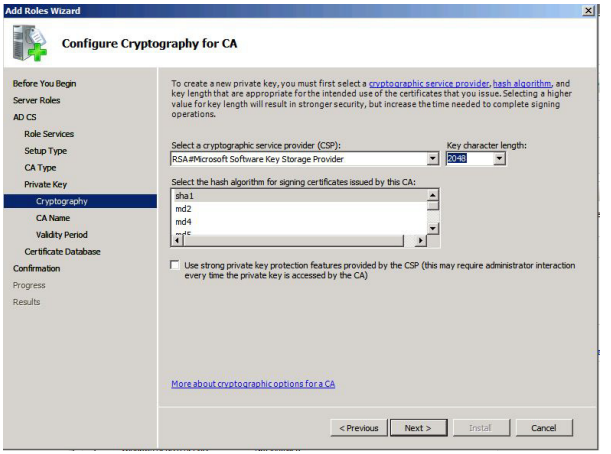

FIGURE D-14. Configure Cryptography for CA screen

11. Click **Next**.
12. On the **Configure CA Name** screen, keep the default settings and click **Next**.
13. On the **Set Validity Period** screen, keep the default settings and click **Next**.
14. On the **Configure Certificate Database** screen, keep the default settings and click **Next**.
15. On the **Confirm Installation Selections** screen, click **Install**.
16. After the installation completes, click **Close**.

Step 2. Generate a Certificate Signing Request (CSR)

1. Go to **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**, and select the server name.
2. Double-click the **Server Certificates** icon.

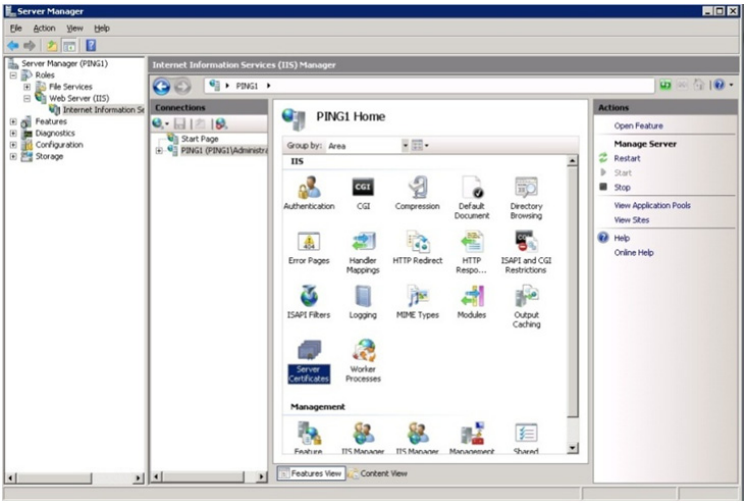

FIGURE D-15. Accessing Server Certificates

Note: The IIS version 7.0 is used to configure SSL certificate in this document.

---

3. From the Actions pane on the right, click **Create Certificate Request**. The **Request Certificate** wizard appears.

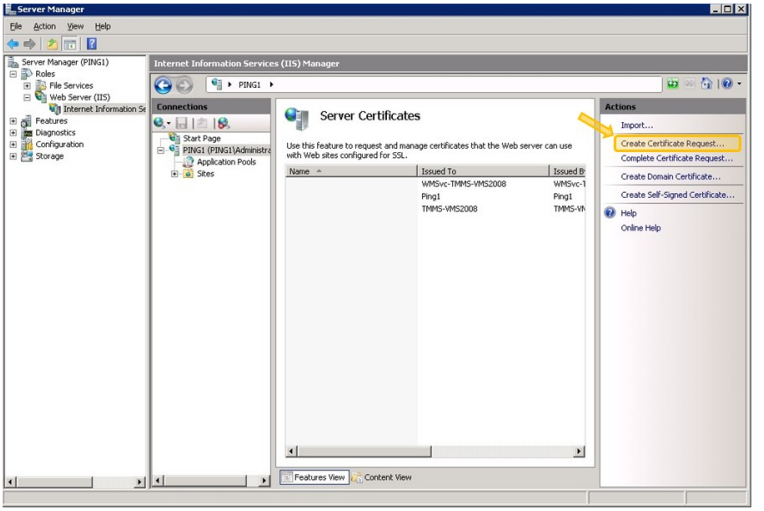

FIGURE D-16. Starting Request Certificate wizard

4. In the **Distinguished Name Properties** window, type the following:
   - **Common name—**the IP address or the registered host name of the Communication Server. For example: `mobile.trendmicro.com`.
   - **Organization—**the legally registered name of your organization/company
   - **Organizational unit—**the name of your department within the organization
   - **City/locality—**the city in which your organization is located
   - **State/province—**the state or province in which your organization is located
   - **Country/region—**the country or region in which your organization is located

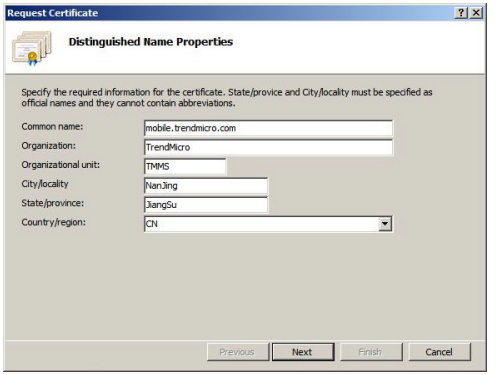

FIGURE D-17. Distinguished Name Properties screen

5. Click **Next**. Cryptographic Service Provider Properties window appears.
6. Select **Microsoft RSA SChannel Cryptographic Provider** in the **Cryptographic service provider** field and **2048** in the **Bit length** field, and then click **Next**.

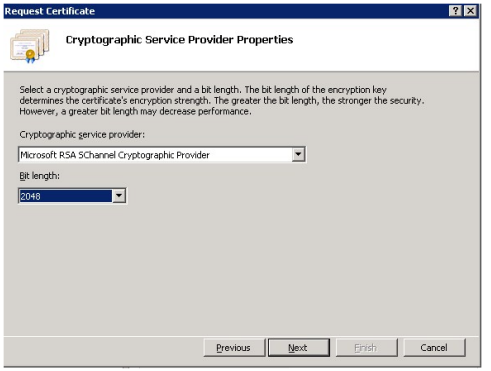

FIGURE D-18. Cryptographic Service Provider Properties screen

7. Select a location where you want to save the certificate request file. Make sure to remember the filename and the location where you save the file.

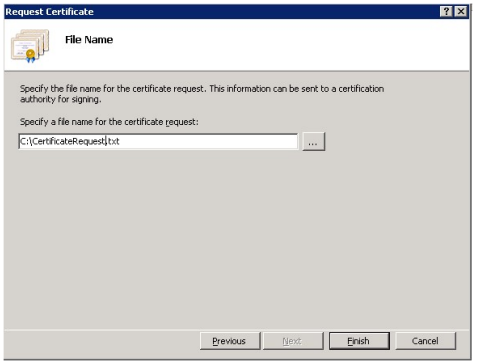

FIGURE D-19. File Name screen

8. Click **Finish**. You have now created a CSR and are ready to sign the SSL certificate.

Step 3. Sign and export the SSL Certificate

1. Go to **Start** > **Administrative Tools** > **Server Manager**, and right-click **Roles** > **Active Directory Certificate Services** > [computer name], and click **Submit new request**.
2. Select the CSR file you created in *Step 2. Generate a Certificate Signing Request (CSR)* and then click **Open**.
3. Click **Roles** > **Active Directory Certificate Services** > [computer name] > **Pending Requests**, and then right-click the request, and select **All Tasks** > **Issue**.

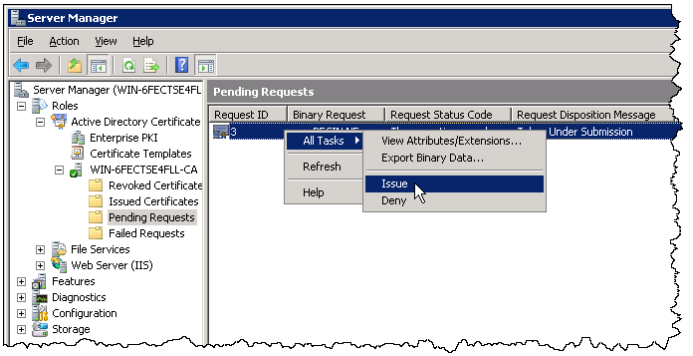

FIGURE D-20. Pending requests in Server Manager

4. Select **Roles** > **Active Directory Certificate Services** > [computer name] > **Issued Certificates**, and double-click the issued certificate. The **Certificate** window displays.

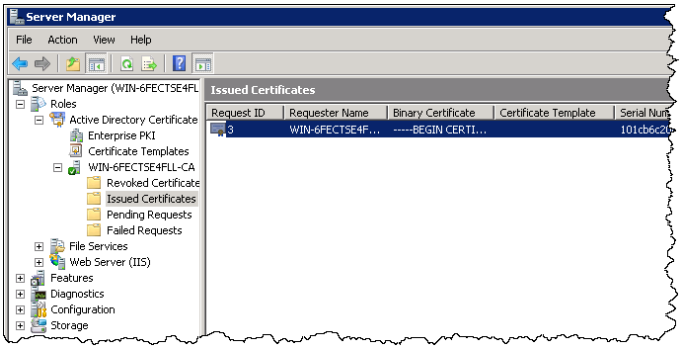

FIGURE D-21. Issued certificates in Server Manager

5. On the **Details** tab, click **Copy to File**. The **Certificate Export Wizard** displays.
6. On the welcome screen, click **Next**.

7. On the **Export File Format** screen, keep the default settings and click **Next**.
8. On the **File to Export** screen, click **Browse** and select the file name and location on your hard drive where you want to save the file.
9. Click **Save**, and then click **Next** on the **File to Export** screen.
10. Click **Finish** to export the SSL certificate. A pop up message displays notifying that the export was successful.
11. On the **Certificate** window, click **Certification Path** tab, select the root certificate, and then click **View Certificate**. The root **Certificate** window pops up.
12. Repeat *Step 5* to *Step 10* of this procedure for the root certificate and click **OK** on the **Certificate** window.

Step 4. Install the SSL certificate on the Communication Server

1. Go to **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**, select the server name, and then double-click **Server Certificates**.
2. From the **Actions** pane on the right, click **Complete Certificate Request**. The Complete Certificate Request wizard appears.

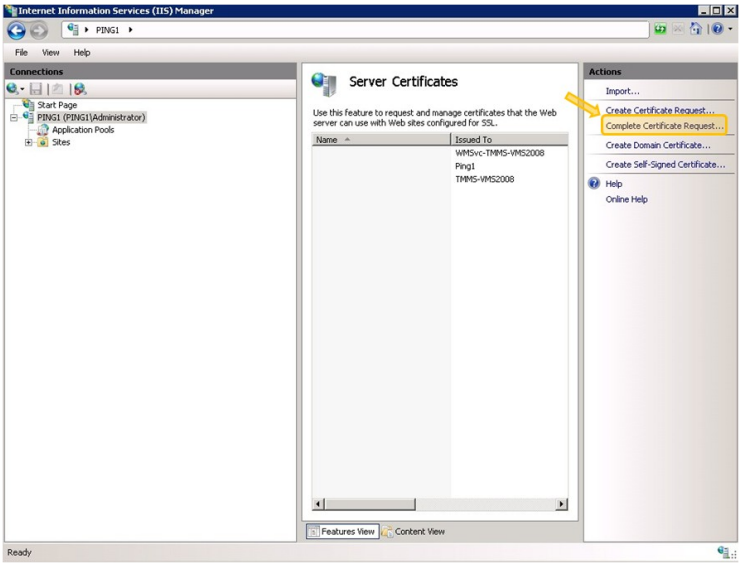

FIGURE D-22. Complete Certificate Request

Note: If you are using IIS 7.5, clicking **Complete Certificate Request** may display the following error message:

A certificate chain could not be built to a trusted root authority.

If this happens, refer to *Configure IIS 7.5 for APNs Certificate Installation starting on page C-15* for the procedure to resolve this issue.

---

3. Select the SSL certificate (`.cer`) file that you have created in *Step 3. Sign and export the SSL Certificate* or purchased in *Step 2. Purchase a public SSL certificate* on page D-13, and type the server IP or host name in the **Friendly name** field. The server IP or host name should be the same as the **Common name** you provided while creating the CSR. Click **OK**.
4. From the **Connections** pane, select [server name] > **Sites** > **OfficeScan**.

Note: If OfficeScan does not appear in the **Connections** pane, select [server name] > **Sites** > **Default Web Site**.

5. From the **Actions** pane on the right, click **Bindings**. The **Site Bindings** pop-up window displays.
6. Select **https** and click **Edit**. The **Edit Site Binding** pop-up window displays.
7. From the **SSL certificate** drop-down menu, select the SSL certificate you created in *Step 3* of this procedure and click **OK**.
8. Click **Close** on the **Site Bindings** pop-up window.
9. Restart IIS.

Step 5. Install SSL certificate on iOS mobile devices

1. Install the root certificate on your computer by performing the following steps:
   a. Double-click the root certificate, and then on the **Certificate** window, click **Install Certificate**.
   b. On the welcome screen, click **Next**.
   c. Keep the default setting, and click **Next**.
   d. Click **Finish** to start the installation. A pop up message displays notifying that the certificate import was successful.
2. Download and install the iPhone Configuration Utility from the following URL:

   http://support.apple.com/downloads/
3. Create a profile for iOS mobile devices:
   a. Start the **iPhone Configuration Utility** and click **Configuration Profiles** from the **Library** list on the left.
   b. Click **New** to add a new profile in the profiles list.
   c. Select the new profile that you have created, then select **Credentials** from the center pane, and then click **Configure** on the **Configure Credentials** on the right pane. The **Personal Certificate Store** displays.
   d. Select the root certificate from the list and then click **OK**.
   e. Click **General** on the center pane and then on the **Identity** area, type the relevant information in all the text fields provided.

4. Install the profile on the iOS mobile device:
   a. Connect the iOS mobile device to the computer where you have installed the root certificate.
   b. Select the iOS mobile device from the **Devices** list on the left.
   c. On the **Configuration Profiles** tab, select the profile you just created, and then click **Install**. The **iPhone Configuration Utility** pushes the profile to the mobile device.
   d. On the mobile device, tap **Install** on the Install Profile screen and then tap **Install Now** on the Root Certificates pop message. The profile installation starts.
   e. After the profile is installed, tap **Done** on the Profile Installed screen.

Obtaining and Installing a Public SSL Certificate on Communication Server

This section provides the procedure of obtaining and installing a public SSL certificate for HTTPS for iOS mobile devices.

The following are the basic steps for obtaining and installing a public SSL certificate:

1. Generate a Certificate Signing Request (CSR).
2. Purchase a public SSL certificate from an SSL certificate provider.
3. Install the purchased certificate in IIS manager on the Communication Server.

Step 1. Generate a Certificate Signing Request (CSR)

Refer to *Step 2. Generate a Certificate Signing Request (CSR)* on page D-5 for the procedure of generating a public SSL certificate. After completing this procedure you will be ready to purchase a public SSL certificate.

Step 2. Purchase a public SSL certificate

Purchase a public SSL certificate from an SSL certificate provider using your CSR file you generated in *Step 1*, and save it as a `.cer` file.

Step 3. Install the purchased certificate in IIS manager on the Communication Server

Refer to *Step 4. Install the SSL certificate on the Communication Server* on page D-10 to import the purchased certificate in IIS manager.

Step 4. Upload SSL certificate to sign iOS client profile (optional)

If you use SSL certificate to sign the iOS client profile, the profile will display the sign status as **`Verified`**. This will not effect any of the other operations, settings or configurations.

To upload SSL certificate to sign iOS client profile:

1. Log on to the OfficeScan Web console and click **Plug-in Manager**.
2. Click **Manage Program**.
3. Click **Administration** > **Communication Server Settings**.
4. On the **iOS Settings** tab, do the following:
   a. In the **Client Profile Signing Credential** section, select **Upload a new credential** from the dropdown list. The **Add certificate** pop-up window appears.
   b. Click **Browse**, select the SSL certificate, and then click **Save** to upload the certificate and close the window.
5. Click **Save** on the Communication Server **Settings** screen.

Generating and Configuring SSL Certificate in Windows 2003 Server Using IIS 6.0

Refer to the following URL for the detailed steps on generating and configuring SSL certificate in Windows 2003 Server using Internet Information Services (IIS) 6.0:

http://esupport.trendmicro.com/solution/en-us/1060664.aspx

TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: TSEM85685/120925