Table of Contents

About this guide

This guide is intended to help users to get the best productivity out of the product. It contains a collection of best practices which are based on knowledge gathered from previous enterprise deployments, lab validations, and lessons learned in the field.

Examples and considerations in this document provide guidance only and do not represent restrict design requirements. The guidelines in this document do not apply to every environment but will help guide you through the decisions that you need to configure Trend Micro Mobile Security for optimum performance.

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme file and the latest version of the applicable user documentation.

This document is designed to be used in conjunction with the following guides, all of which provide more detail about Trend Micro Mobile Security than are given here:

Trend Micro Mobile Security 9.8 SP3 for Enterprise Installation and Deployment Guideline
http://docs.trendmicro.com/all/ent/tmms-ee/v9.8_sp3/en-us/tmms-ee_9.8_sp3_idg.pdf

Trend Micro Mobile Security 9.8 SP3 for Enterprise Administrator’s Guide
http://docs.trendmicro.com/all/ent/tmms-ee/v9.8_sp3/en-us/tmms-ee_9.8_sp3_fvdm_ag.pdf

The latest IDG and AG version can be found in downloadcenter.trendmicro.com

This document contains

- Deployment considerations and deployment
- Guidance in sizing server and storage sources for Trend Micro Mobile Security 9 for Enterprise implementation
- Upgrade guidelines and scenarios
- Configuration recommendations to maximize system performance and reduce administrative overhead

Acknowledgements

This guide was made possible by the following individuals who volunteered their time and expertise to this project.

<Author/s>
Second Chen, Annie Ye, April Xu

Document version: 1.0
Release Date: 2019/12/31

Chapter 1: Environment

1.1 > Operating Systems

Component	Requirements
Management Server And Communication Server	• Windows 2012 Server Family • Windows 2012 R2 Server Family • Windows Server 2016 • Windows Server 2019
	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
Microsoft Exchange Server	• Microsoft Exchange 2007 • Microsoft Exchange 2010 • Microsoft Exchange 2013
Mobile Security Exchange Connector	Platform • Windows 2008 R2 Server (64-bit) • Windows 2012 • Windows 2012R2 Hardware • 1-GHz Intel™ Pentium™ processor or equivalent • At least 1 GB of RAM • At least 200 MB of available disk space Software • .Net 3.5sp1

1.2 > Database Systems

Component	Requirements
Microsoft SQL Server	• Microsoft SQL Server 2012/2012 Express Edition • Microsoft SQL Server 2016/2016 Express Edition • Microsoft SQL Server 2017/2017 Express Edition

1.3 > Internet Information Services

Component	Requirements
IIS Web Server for Management Server	Microsoft Internet Information Services (IIS) 8.0/9.0/10.0

	↳ The IIS is an integral part of Microsoft Windows and the IIS version corresponds to the Windows version installed. ↳ Keep the default settings and select. When using IIS 7.0 or above the default settings and enable | install **CGI** and **ISAPI Extensions** in Application Development, **HTTP Redirection** in Common HTTP Features, and **IIS6 Management Compatibility** in Management Tools ↳ Trend Micro Mobile Security does NOT support Apache Web Server

1.4 > Web Browser

Component	Requirements
Web Browser	• Internet Explorer 9 or above • Chrome 57 or above • Firefox 54 or above • Safari 10 or above on Mac ↳ ADOBE Flash Player is required for the Mobile Security administration web console

1.5 > Agents

Component	Requirements
Android	• Memory 28MB • Storage 14MB
IOS	• Memory 17MB • Storage 12MB

Chapter 2: Sizing Considerations

2.1 > Server Sizing

Devices	Management Server	Local Communication Server (if used)	SQL Server	Data Sizes
5000	4 vCPU， 2GB RAM	2 vCPU， 2GB RAM	4 vCPU， 8GB RAM	**Devices**: 0.1MB each device **Policies**: 0.2MB each policy **Event logs**: 10000 event logs occupy about 2MB; 5 event logs (1KB) for each device per day. **Command queues**: 10000 commands for Android occupy about 3MB, for iOS occupy about 30MB; 5 commands per day (for Android about 1.5KB, for iOS about 15KB)
10000	4 vCPU， 4GB RAM	2 vCPU， 4GB RAM	8 vCPU， 12GB RAM	

Note: vCPU means a CPU Core with Intel 2GHZ+

2.2 > Recommendation

- To have better UI performance and better request/command performance, please contain limited devices (less than 2000) for each group.
- For policy sync, we suggest change policies by group; not by root group and apply all.
- After enrollment, one device will use less than 0.1 MB database storage but there will be more and more data (mostly device logs) in the future.
- Please wait for at least 15 ~20 minutes to change different groups` policy if the number of devices is large in groups.
- At least 50GB hard disk for database storage, it depends on the device volume

  We also recommend the customer use a dedicate server to install TMMS 9.3 and later versions.

  Although TMMS 9.2 support installation with OfficeScan and TMCM, but it may cause some potential issues. E.g. Install OfficeScan server with Apache, then install TMMS 9.2 on same server, the PHP may only bind to Apache. When this issue happens, please migrate OfficeScan from Apache to IIS, because TMMS 9.2 only support IIS. TMMS 9.3 and later versions has resolved the problem.

Chapter 3: Installation and Deployment

3.1 > Database Server

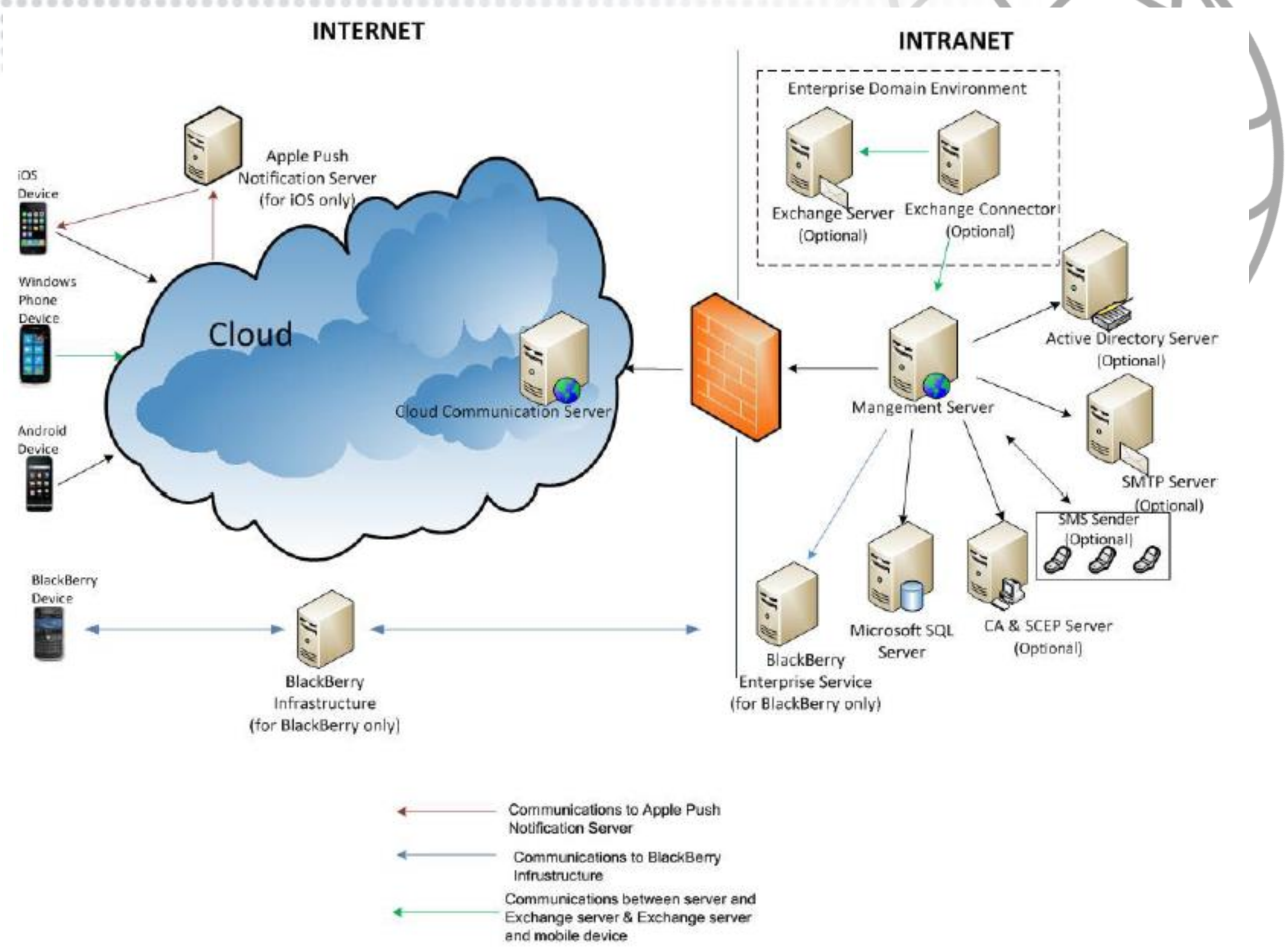
Trend Micro Mobile Security only supports Microsoft SQL server. By default, during installation of TMMS it also installs SQL Server Express 2017.

Microsoft SQL Server
http://en.wikipedia.org/wiki/Microsoft_SQL_Server

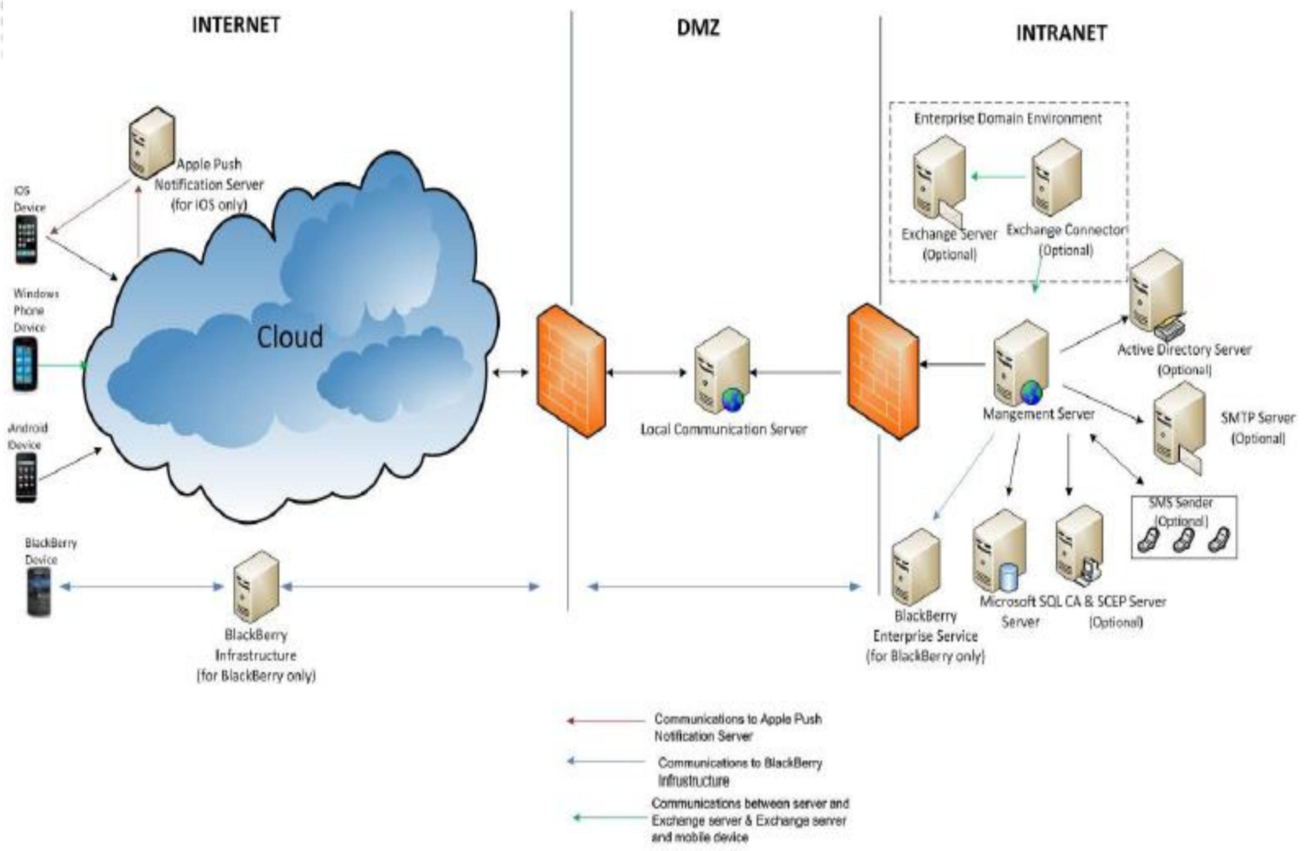
SQL Server Best Practice Guide
http://technet.microsoft.com/library/Cc966412

3.2 > Deployment Type

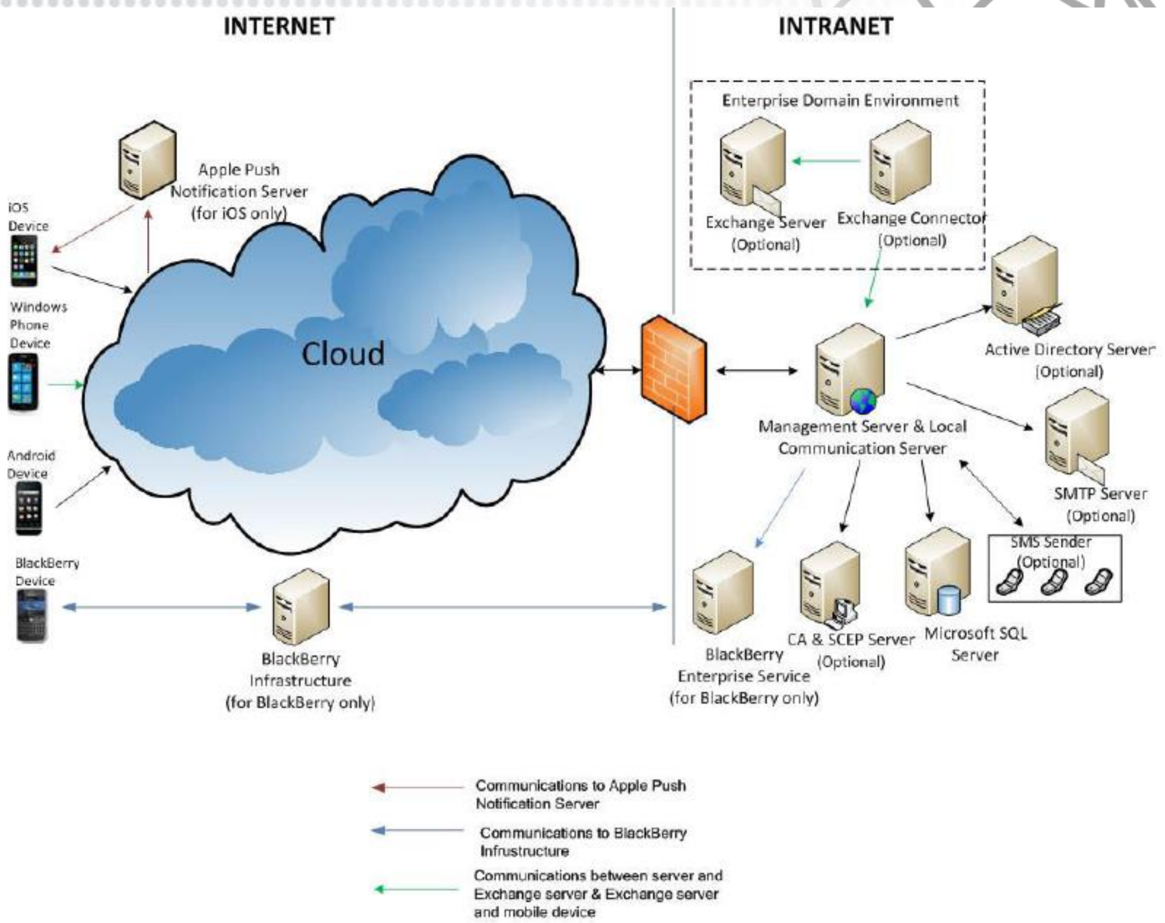
Trend Micro recommends below deployment types that will help with the strategically distribution of servers on the network environment to better facilitate mobile and security policy management as well with the implementation of client to server communication.
Enhanced Security Model (Dual Server Installation) with Cloud Communication
Server



Enhanced Security Model (Dual Server Installation) with Local Communication Server


INTERNET
DMZ
INTRANET
Apple Push Notification Server (for IOS only)
IOS Device
Windows Phone Device
Android Device
Cloud
BlackBerry Device
BlackBerry Infrastructure (for BlackBerry only)
Local Communication Server
Enterprise Domain Environment
Exchange Server (Optional)
Exchange Connector (Optional)
Mangement Server
Active Directory Server (Optional)
SMTP Server (Optional)
SMS Sender (Optional)
BlackBerry Enterprise Service (for BlackBerry only)
Microsoft SQL Server
CA & SCEP Server (Optional)
Communications to Apple Push Notification Server
Communications to BlackBerry Infrustructure
Communications between server and Exchange server & Exchange server and mobile device

Basic Security Model (Single Server Installation)


INTERNET
INTRANET
Enterprise Domain Environment
Exchange Server (Optional)
Exchange Connector (Optional)
Apple Push Notification Server (for iOS only)
iOS Device
Windows Phone Device
Android Device
BlackBerry Device
Cloud
BlackBerry Infrastructure (for BlackBerry only)
Active Directory Server (Optional)
Management Server & Local Communication Server
SMTP Server (Optional)
SMS Sender (Optional)
BlackBerry Enterprise Service (for BlackBerry only)
CA & SCEP Server (Optional)
Microsoft SQL Server
Communications to Apple Push Notification Server
Communications to BlackBerry Infrustructure
Communications between server and Exchange server & Exchange server and mobile device

Enhanced Security Model (Dual Server Installation) with Cloud Communication Server

- Choose whether to install a Local server communication (LCS) or utilize Trend Micro's cloud communication server (CCS).

Features	Cloud Communication Server	Local Communication Server
Installation required	No	Yes
User authentication method supported	Enrollment Key	Active Directory or Enrollment Key
Agent Customization for Android	Supported	Supported
Manage Windows Phone devices	Not supported	Supported

- For LCS deployment, you will need a valid SSL certificate or use self-signed certificate.
- Choose between the integrated or stand-alone SQL Server. Stand-alone SQL server is recommended for production environment.
- APNs certificate is required if you want to manage IOS mobile devices.

3.3 > Network Ports

Please refer to the Installation and Deployment Guide, **Appendix A Network Ports Configurations** for detailed information.

3.4 > Certificates

A certificate is a document that your website shows a browser to contain proclaiming its identity. It is basically, tells that who is what it says it is. It contains the organizations' domain name and identification such as company's name, address and so forth. But in order to trust a certificate, it has to be signed by a Certificate Authority.
For more information, please see this link:
http://en.wikipedia.org/wiki/Public_key_certificate
What are the needed certificates to make Trend Micro Mobile Security for Enterprise to work?
For iOS, it is required to have an Apple Push Notification Services Certificate in order to manage an iOS device. This has been Apple requirement which is NOT limited to Trend Micro Mobile Security for Enterprise but to other 3rd party MDM applications as well.

Apple Push Notification Services Certificate
Public or Private SSL Certificate – Certification Authority Services

For Android, either a Public or Private SSL certificate will do. Although it does not really required, since TMMS devices or MDAs can communicate through either HTTP or HTTPS.

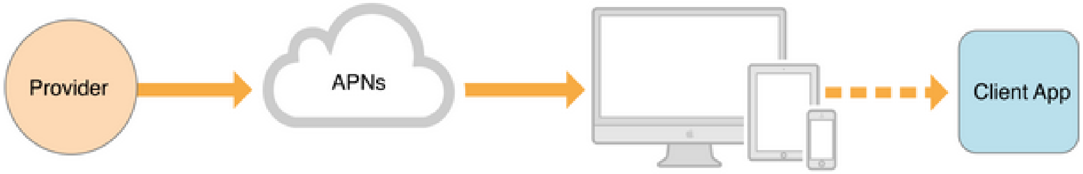
3.4.1.1 Apple Push Notification Services

The Apple Push Notification Service is a service created by Apple Inc. that was launched together with iOS 3.0 on June 17, 2009. It uses push technology through a constantly open IP connection to forward notifications from the servers of third party applications to the Apple devices; such notifications may include badges, sounds or custom text alerts. In iOS 5, Notification Center enhanced the user experience of push and local notifications. APNs was also added as an API to Mac OS X v10.7 "Lion" for developers to take advantage of, and was greatly improved in OS X 10.8 "Mountain Lion" with the introduction of Notification Center.

Please read more, see link below:
http://en.wikipedia.org/wiki/Apple_Push_Notification_Service

https://developer.apple.com/library/ios/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/Chapters/ApplePushService.html

Here is a basic push notification from a provider (MDM server – Trend Micro Mobile Security for Enterprise) to a client (Mobile Device Agent / MDA) application.



3.4.2.1 Public SSL Certificate

What are the advantages of an external or public Certificate Authority (CA)?

- The external Certificate Authority (CA) is responsible of the security and accountability of the Public Key Infrastructure or PKI.
- External parties trust a digital certificate signed by a trusted Certificate Authority (CA) such as Verisign, Thawte, Comodo, Godaddy, etc.

What are the disadvantages of an external or public Certificate Authority (CA)?

- Integration of external Certification Authority (CA) and the infrastructure of the organization are limited.
- The organization has to pay for the certificate when you are using the service of an external Certification Authority (CA).
- Flexibility of when configuring, expanding and managing certificates. Organization must contact external Certification Authority (CA).

3.4.3.1 Private SSL Certificate

What are the advantages of using an internal or private Certificate Authority (CA)?

- The ease of management is the main advantage - as you can manage certificates such as revoking or issuing. No need to contact an external or public certificate authority.
- An internal or private Certificate Authority can be integrated with Active Directory which make ease of the Certificate Authority structure.
- There is no cost of using of using an internal o private Certificate Authority
- The auto-enrollment feature of Windows Server 2003 and later versions further simplifies the certificate issuing process.

What are the disadvantages of using an internal or private Certificate Authority (CA)?

- Implementing internal or private Certificate Authority (CA) is complicated as to having or using an external Certificate Authority (CA).
- The security and accountability of Public Key Infrastructure (PKI) is completely on the organization.
- External parties will not trust a certificate signed by an internal Certificate Authority (CA).

3.4.4.1 TMMS related certificates.

TMMS 9.x need 2 certificates
3.3.4.1.1 APNS certificate

The first one is APNS certificate, this certificate is used for LCS/CCS server to communicate with Apple Push Network Service. The expired date of this certificate is 1 year.
Please refer to the Installation and Deployment Guide for detailed apply and renew instructions.

3.3.4.2 LCS/CCS certificate
The second one is LCS/CCS certificate. This certificate is used for Agent connect to LCS/CCS.
For CCS, TrendMicro has already applied a publish certificate for the server.
For LCS, the administrator need to apply a new public certificate with the **LCS FQDN or IP address**, please keep integrate with Web console's "Common Settings->External domain name or IP address", E.g. the LCS's FQDN (Fully Qualified Domain Name) is lcs.trendmicro.com, then the administrator need to apply for the certificate with "lcs.trendmicro.com ". LCS also support self-signed certificate. While the administrator installs LCS, please set the name as FQDN.

Most public certificates will be issued by an intermediate authority that has been issued by a root authority. To make LCS support the certificate, you need to include root CA and intermediate CA in the PFX certificate for LCS
For details, please refer http://esupport.trendmicro.com/solution/en-us/1106466.aspx

If the network environment contains NAT, please give the public IP address or the public FQDN while create the certificate.

3.4.5.1 Changing SSL Certificate after Installation (CertConfigTool.exe)

Here are the steps:
1. On the TMMS server, navigate to drive: \Program Files (x86)\Trend Micro\Communication Server directory.
2. Right click CertConfigTool.exe and choose Run as Administrator.
3. Choose the option: Import an existing .pfx or .p12 certiicate file
4. Click Next.
5. On the "Certificate file:" click Browse... and then point to the latest CA.pfx we generated.
6. Enter the Password:
7. Leave "CA certificate:" blank.
8. Click Next.
9. You should see the message: Communication Server configuration file updated successfully.
10. Click Finish.
11. Restart "Mobile Security Communication server" service

3.5 > Devices

3.5.1 Android Device

You can install the MDA for Android mobile devices using one of the following methods:

- **Installation Method I—Download and install the MDA from google play.**
  Open the mobile device, open "Google play store"

Search for Trend Micro Enterprise Mobile Security, and tap Enterprise Mobile Security from the search results.
Tap Install, and then tap Accept to start the installation process.
After the installation process completes, tap the Open to start the application.

- **Installation Method II—Download and install the MDA directly on a mobile device.**
  Access one of the following URLs using a Web browser on the mobile device where you want to install the MDA to download the installation package:
  http://External_domain_name_or_IP_address:HTTP_port/mobile
  or
  https://External_domain_name_or_IP_address:HTTPS_port/mobile
  If the installation does not start automatically, launch the installation package and complete the installation.
- **Installation Method III—Download the MDA installation package on a computer using a Web browser, then transfer it to the mobile device and install.**
  On a computer, navigate to one of the following URLs to download the installation package:
  http://External_domain_name_or_IP_address:HTTP_port/mobile
  Select the operating system of the mobile device to download the installation package.
  Copy the installation package to the mobile device.
  Launch the installation package and complete the installation.
- **Installation Method IV—Download the MDA installation package on a computer using Mobile Device Management console, then transfer it to the mobile device and install.**
  Click Administration → Device Enrollment Settings.
  On the Agent Installation tab, select the agent installation package and click Download to download the ZIP file to your computer.
  Extract the ZIP file and copy the installation package to the mobile device.
  Launch the installation package and complete the installation.

NOTE: The default invitation email message sent to the users instruct the users to download and install the MDA app from Google Play store (Method I). If you want to use another method for users to install the app, modify the invitation email message sent to the users. Refer to the topic Configuring Installation Message in IDG document.

3.5.2 Apple Device

You can install the MDA for iOS mobile devices from the Apple store. To download and install the MDA, go to the Apple store, search for the app *Trend Micro ENT Security*, and tap **Install**.

Chapter 4: Configuration

4.1 > UI

Web console (Internet Explorer 8.0 or above, Chrome 17 or above, Firefox 14 or above, Safari 6 or above on Mac)

-Using Internet Explorer, make sure to:
a. Turned off Compatibility View for Web Sites
b. The JavaScript is enabled in browser
c. Disable Enhanced Protected Mode is using Windows 2012 and Windows 2012 R2

4.2 > Dashboard

The **Dashboard** screen displays first when you access the Management Server. This screen provides an overview of the mobile device registration status and component details.
The dashboard screen is divided into five tabs:

- *Summary*—shows the device health status and device's operating system summary.
- *Health*—shows the components and policy update and mobile device health status. In this category, you can:
  - View mobile devices' status:
    - *Healthy*—shows that the device is enrolled to the Mobile Security server and the components and policies on the mobile device are up-to-date.
    - *Non-Compliant*—shows that the device is enrolled to the Mobile Security server, but does not comply with the server policies.
    - *Out of Sync*—shows that the device is enrolled to the Mobile Security server, but either the components or the polices are out-of-date.
    - *Inactive*—shows that the device is not yet enrolled to the Mobile Security server.
  - View the total number of enrolled and unregistered mobile devices managed by Mobile Security.

    A mobile device may remain unregistered if one of the following happens:

    - a connection to the Communication Server is unsuccessful
    - the mobile device user has deleted the registration SMS message
  - View mobile device program patch and component update status:
    - *Current Version*—the current version number of the Mobile Device Agent or components on the Mobile Security server
    - *Up-to-date*—the number of mobile device with updated Mobile Device Agent version or component
    - *Out-of-date*—the number of mobile devices that are using an out-of-date component
    - *Update Rate*—the percentage of mobile devices using the latest component version
    - *Upgraded*—the number of mobile devices using the latest Mobile Device Agent version
    - *Not Upgraded*— the number of mobile devices that have not upgraded to use the latest Mobile Device Agent version

        - *Upgrade Rate*—the percentage of mobile devices using the latest Mobile Device Agent
    - View server update status:
        - *Server*—the name of the module
        - *Address*—the domain name or IP address of the machine hosting the module
        - *Current Version*—the current version number of the Mobile Security server modules
        - *Last Updated*—the time and date of the last update
- *Inventory*—shows mobile device operating system version summary, telephone carriers summary, mobile device vendors summary and top 10 applications installed on mobile devices.
- *Compliance*—shows the app control, encryption and jailbreak/root status of mobile devices. In this category, you can:
    - View the mobile device jailbreak/root status:
        - *Jailbroken/Rooted*—the number of mobile devices that are jailbroken/rooted
        - *Not Jailbroken/Rooted*—the number of mobile devices that are not jailbroken/rooted
    - View the mobile device encryption status:
        - *Encrypted*—the number of mobile devices that are encrypted
        - *Not Encrypted*—the number of mobile devices that are not encrypted
    - View the mobile device application control status:
        - *Compliant*—the number of mobile devices that comply with the Mobile Security's compliance and application control policy
        - *Not Compliant*—the number of mobile devices that do not comply with the Mobile Security's compliance and application control policy
- *Protection*—shows the lists of top five (5) security threats and top five (5) blocked Web sites.

4.3 > Devices

4.3.1 Mobile Device Groups

Mobile Security server automatically creates a root group *Mobile Devices* with the following two sub-groups:

- *default*—this group contains Mobile Device Agents that do not belong to any other group. You cannot delete or rename the *default* group in the Mobile Security device tree.
- *unauthorized*—Mobile Security server automatically creates this group if *Device Authentication* is enabled in **Device Enrollment Settings**, and a list of mobile devices is used to authenticate. If there is an enrolled mobile device that is not in the list of mobile devices, Mobile Security moves such mobile device to the *unauthorized* group. Mobile Security also creates other groups and regroups all mobile devices according to the list that you use.

  Note: Please don't add more than 3000+ devices to a group, this will cause performance issue while expand the group

4.3.2 Mobile Device Agent Tasks

Trend Micro Mobile Security enables you to perform different tasks on the mobile devices from the **Devices** screen.

Sending Invitation to Mobile Devices
Editing Mobile Device Information

Deleting Single Mobile Device
Deleting Multiple Mobile Devices
Moving Mobile Devices to Another Group
Updating Mobile Device Agents
Lost Device Protection
Resetting Password Remotely
Exporting Data
Sending Messages to Mobile Devices

4.4 > Policies

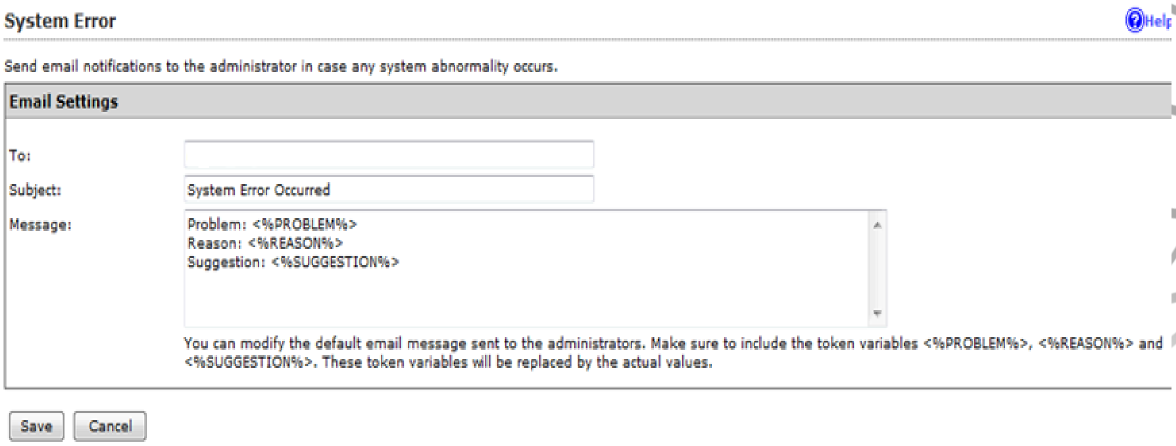
You can configure security policies for a Mobile Security group on the Management Server. These policies apply to all mobile devices in the group. You can apply security policies to all Mobile Security groups by selecting the *Mobile Devices* group (the root group). The following table lists the security policies available in Mobile Security.

Security Policies in Mobile Security

Policy Group	Policy
General	Common Policy
Provisioning	Wi-Fi Policy
	Exchange ActiveSync Policy
	VPN Policy
	Global HTTP Proxy Policy
	Certificate Policy
	Single Sign-On Policy
	AirPlay/AirPrint Policy
	Cellular Network Policy
	Theme Policy
Device Security	Malware Protection Policy
	Spam Prevention Policy
	Call Filtering Policy
	Web Threat Protection Policy
Devices	Password Policy
	Feature Lock Policy
	Compliance Policy
Application Management	Application Monitor & Control Policy
	Volume Purchasing Program Policy
Samsung KNOX	Container Policy

4.5 > Notifications

TMMS will send different System Error Notification Events to the Administrator.



System Error

Send email notifications to the administrator in case any system abnormality occurs.

Email Settings

To:

Subject: System Error Occurred

Message:

```
Problem: <%PROBLEM%>
Reason: <%REASON%>
Suggestion: <%SUGGESTION%>
```

You can modify the default email message sent to the administrators. Make sure to include the token variables <%PROBLEM%>, <%REASON%> and <%SUGGESTION%>. These token variables will be replaced by the actual values.

Below are the Error lists

System Error Notification Event	Description
MAIL_PROBLEM_SCEP_AFTER	Unable to retrieve the challenge password from SCEP server.
MAIL_REASON_SCEP_AFTER	The SCEP server is inaccessible.
MAIL_SUGGESTION_SCEP_AFTER_RERLACE	Make sure that the SCEP server is alive and the policy server can access its Web server.
MAIL_PROBLEM_SCEP_AUTH_AFTER	Unable to retrieve the challenge password from SCEP server.
MAIL_REASON_SCEP_AUTH_AFTER	The policy server authentication fails.
MAIL_SUGGESTION_SCEP_AUTH_AFTER	Check the SCEP server settings to make sure they are correct, and try again.
MAIL_PROBLEM_SCEP_PASS_AFTER	SCEP server returned an invalid challenge password.
MAIL_REASON_SCEP_PASS_AFTER	The SCEP server's pool is full.
MAIL_SUGGESTION_SCEP_PASS_AFTER	Increase the SCEP server's pool size, and try again.
MAIL_PROBLEM_NOTI_APNS_AFTER	Unable to send APNs push notification message.
MAIL_REASON_NOTI_APNS_AFTER	The Apple Push Notification service is unreachable.
MAIL_SUGGESTION_NOTI_APNS_AFTER	Make sure that the Policy Server can connect to gateway.push.apple.com and your APNs certificate is valid, and try again.
MAIL_PROBLEM_SENDER_AFTER	Unable to send text message.
MAIL_REASON_SENDER_AFTER	Mobile Security is unable to access the SMS sender.

System Error Notification Event	Description
MAIL_SUGGESTION_SENDER_AFTER	Make sure that the SMS sender is connected to the Master Server, and try again.
MAIL_PROBLEM_LDAP_AFTER	Unable to connect to the LDAP server.
MAIL_REASON_LDAP_AFTER	The settings are incorrect or the account is expired.
MAIL_SUGGESTION_LDAP_AFTER_RERLACE	Check the LDAP settings, and try again.

4.6 > SCEP and TMMS built-in SCEP schema

We recommend **NOT** use SCEP; this is inherited from OLD TMMS version.
What is Simple Certificate Enrollment Protocol?

Simple Certificate Enrollment Protocol is an Internet Draft in the Internet Engineering Task Force (IETF). This protocol is being referenced by several manufacturers of network equipment and software who are developing simplified means of handling certificates for large-scale implementation to everyday users.

The protocol is designed to make the issuing and revocation of digital certificates as scalable as possible. The idea is that any standard network user should be able to request their digital certificate electronically and as simply as possible. These processes have usually required intensive input from network administrators, and so have not been suited to large scale deployments.

SCEP is the most popular, widely available and most tested certificate enrollment protocol. It has several advantages over competing protocols [citation needed], such as Certificate Management Protocol.

See reference link below to know more (about SCEP, CA, NDES, etc.)

http://en.wikipedia.org/wiki/Simple_Certificate_Enrollment_Protocol
http://technet.microsoft.com/en-us/library/cc755071.aspx

Trend Micro Mobile Security for Enterprise has a feature where you can use Microsoft SCEP (an option if the company would like to manage and distribute their own SSL certificate).

For more information, please see link below:
http://technet.microsoft.com/en-us/windowsserver/dd448615.aspx

What is the role of MS SCEP to Trend Micro Mobile Security for Enterprise?

4.7 > Microsoft Exchange ActiveSync

The Exchange ActiveSync protocol allows mobile devices running Windows Mobile to synchronize e-mail, calendar, contacts, and tasks (known as PIM, Personal Information Manager) over the air with the Microsoft Exchange Server.

The sync protocol is the language spoken between the mobile device and messaging server to synchronize objects. The device will have its own e-mail, contacts, calendar and task (PIM – Personal Information Manager) application, which provides a user interface and data storage. Syncing is the process of reconciling differences between data stored on the mobile device and stored on the Exchange Server.

Both the mobile device and the Exchange Server maintain their own collections of objects and track changes made since the last sync. The mobile device may initiate a new sync by sending a set of updates to the Exchange Server and requesting the Exchange Server respond with its own updates. The Exchange server processes updates it receives, resolves any conflicts, and sends its list of changes back to the mobile device.

In Trend Micro Mobile Security for Enterprise, it provides integration with the Microsoft Exchange Server which supports iOS, Android and Windows Phone mobile devices that uses Exchange ActiveSync service. Trend Micro Mobile Security Exchange Connector connects to Microsoft Exchange server easing the hassles of managing multiple tools and consoles. Once configured and enabled, Exchange ActiveSync feature can send invitation and unmanaged devices, allow or block access to Exchange ActiveSync server, on-demand remote wipe, cancel remote wipe command remove mobile devices from the list.

4.8 > Deployment Settings

Refer to the following Knowledge Base article about switching from Full Version deployment mode to Security Scan deployment mode:

Chapter 5: Bandwidth Utilization

5.1 > Agent

Recommend data: 0.1MB each device

Including following major traffics

Agent->CCS, Device Register, 100K bytes

Agent ->CCS, Log upload, 0.2K per log, normally, we consider 5 Logs per device, which is 1K

Agent->AU, Update pattern, it depends on the pattern size

Agent<-CCS, Policy Push, 20KB each policy

Agent<-CCS, Command Push, 0.3KB each policy for Android, 3KB for iOS, 5 commands per day

5.2 > MDM Server

Recommend data: 0. 1MB * Device Number* factor

Factor: This depends on the peak time, how many mobile agents will connect MDM server at the same time,

Including following major traffics

MDM->CCS, HTTP connection Keep Alive 4K bytes / 90 seconds

MDM<->CCS, MDM Agent register 100K bytes /Depends on how many devices will be registered at same time

MDM<->CCS, Log collection, 0.2K bytes, 5 logs per device per day

MDM->CCS, Push APNS certificate to CCS server 5K bytes

MDM->CCS, Policy Push, 20K bytes

MDM->CCS, File transfer, E.g. pattern file, application files that customer upload to the "App Store", Depends on application size.

Chapter 6: Performance Tuning and Optimization

6.1 > Internet Information Services (IIS)

If you have a large number of agent installed, please adjust following parameter to enlarge the IIS supported connections

1. Modify IIS application pool Queue length
   Open IIS Manager > ApplicationPools > MDMAppPool > Advanced Settings
   Queue Length : 65535

2. Adjust IIS appConcurrentRequestLimit, Change it from 5000 to 100000。
   Open IIS Manager->Click "Default Web Site"->Configuration Editor->choose section as "system.webServer/serverRuntime"->Set appConcurrentRequestLimit to 100000->click Apply
3. Adjust TCP connection, Change it from 5000 to 100000。
   reg add HKLM\System\CurrentControlSet\Services\HTTP\Parameters /v MaxConnections /t REG_DWORD /d 100000

4. Modify ASP.Net Request Queue Limit --New added
   For x64 environment, In the Run dialog box, type "notepad %systemroot%\Microsoft.Net\Framework64\v2.0.50727\CONFIG\machine.config", and then click OK.
   Locate the processModel element that looks like this: <processModel autoConfig="true" />
   Replace the processModel element with the following value: <processModel enable="true" requestQueueLimit="100000" />
   Save and close the machine.config file.
   For x86 enviroment, do the same thing for %systemroot%\Microsoft.Net\Framework\v2.0.50727\CONFIG\machine.config

6.2 > Exclude Database from Anti-malware scans

If you have an anti-malware installed on the SQL server, it is strongly suggested to exclude particular SQL directories so that scanning will not hinder its performance, database/s should not be scanned. Since Microsoft SQL Server databases are dynamic, exclude the directory and backup folders from the scan list. If it is necessary to scan the database files, a scheduled task can be created to scan them during off-peak hours.

Directories such as:

```
${ProgramFiles}\Microsoft SQL Server\MSSQL\DATA
${ProgramFiles}\Microsoft SQL Server\Log
${Windir}\WinNT\Cluster and Q:\                    # if using SQL Clustering
```

6.3 > Auto-growth and database maintenance

For Microsoft SQL Databases, ensure less auto-growth events moving forward by adjusting the default auto-growth settings to a higher value.

↳ Each time an auto-growth event is performed, SQL Server holds up database processing. This means that processing against that database will be held up until the auto-growth event completed. This could equate to slower response time for other SQL commands that are being processed against the database that is growing

Monitor and perform Database maintenance jobs to ensure things are working normally and to prevent having large fragmented database which could lead to performance issues.

The Command Queue table will become large while use the TMMS for long time.
TMMS 9.x provide a schedule maintenance database option, this feature will automatically remove the successfully executed Command
Please enable this option

□ **Administration > Command Queue Management > Command Queue Maintenance > Enable scheduled deletion of commands**

6.4 > Database indexing

It's recommended to periodically rebuild the index of the database to improve performance.

Indexes are specialized data structures that operate on tables (and sometimes views) in the database engine used to aid in the searching for and sorting of data. Indexes are vital to the database engine returning results quickly.

As data is modified in the underlying tables that the indexes operate on, the indexes become fragmented. As the indexes become more and more fragmented, query times can begin to suffer. The remedy to this situation is to either reorganize or rebuild the index in MS SQL.

Below are some useful links with additional information on how to do this:

Rebuilding SQL Server Indexes
http://www.sql-server-performance.com/tips/rebuilding_indexes_p1.aspx

Index Rebuilding Techniques
http://www.remote-dba.net/t_tuning_index_rebuilding.htm

Chapter 7: Upgrade and Migration

7.1 > Migration

TMMS8.x->TMMS 9.x

TMMS provide a tool to migrate from TMMS 8.0 to TMMS 9.0 Patch 1

TMMS 9.x->TMMS 9.x
We do not recommend using this tool for backup and restoring. TMMS 9.x can be upgraded from a previous version automatically in the background when a higher version is installed.

7.1.1 Pre-Migration

You must have TMMS 8.0/8.0 SP1 installed before upgrading to TMMS 9.0 Patch 1. You must have TMMS 9.0 Patch 1 freshly installed for migration.

- The current version does not support migration from TMMS 8.0 to TMMS 9.0 Patch 1 using Cloud Communication Server. If you use Local Communication Server in TMMS 9.0, you need to install the Local Communication Server on the computer that has the same server address and port with Communication Server 8.0, refer to Step 4: Restoration Of Database And Configuration.
- After migration, take note of the following:
  - All Android devices will receive a notification to upgrade the agent to 9.0 Patch 1. After the upgrade, the device can be managed by the server through the new agent.
  - All iOS devices whose OS version is lower than 7.0 will receive a notification to download the new iOS agent from the app store. An application icon named **TMMS upgrade** will be provisioned to the home screen. When the agent is installed, you need to click the icon in order for the agent to communicate with the server. The TMMS upgrade icon will be deleted automatically after the agents connect to the server.

    There is no need to re-enroll the device and remove or re-install any profile.

  - All iOS devices whose OS version is 7.0 or higher will also receive a notification to download the new iOS agent from the app store; and an application icon named **TMMS upgrade** will be provisioned to the home screen. When the agent is installed, however, you may get error or be prompted to re-install the mdm enrollment profile when clicking the icon (the profile install will simply fail although, since it has already been installed).

    You need to wait for up to 24 hours when the TMMS 9 server will provision another application icon named **TMMS update** on the home screen. You need to click this icon in order for the agent to communicate with the server. The two application icons will be deleted automatically after the agents connect to the server. There is no need to re-enroll the device again and remove or re-install any profile.

  - For iOS devices whose OS version is 6.0 or higher on TMMS 8.0 GM version, there is a known issue: the required application push for uploaded IPA app or external app from Apple Store cannot work due to insufficient rights of the installed MDM profiles. This known issue is fixed in TMMS 8.0 SP1 for new enrolled devices. Due to this known issue, take note of the following impact if the iOS devices are originally enrolled on TMMS 8.0 GM build (even though the TMMS server is already upgraded to TMMS 8.0 SP1):

- When migrating to TMMS 9 Patch 1, the notification for new agent install will not be prompted on these iOS devices. Instead, you need to manually install it from the Apple Store.
- After migration, the required application push for uploaded IPA app or external app from Apple Store will not work on these iOS devices (however, the devices can still install any application from TMMS enterprise app store). To resolve this known issue, you need to re-enroll the devices need to be re-enrolled and re-install the profiles.

7.1.2 Backing up the database and configuration

When you migrate from TMMS version 8.0 to 9.0 Patch 1, you need to back up the files from version 8.0 and then restore the files when TMMS 9.0 Patch 1 has been installed.

The backup files include:

- Database backup file - backup of version 8.0 database
- Configuration backup files - backup of version 8.0 configuration files on the Management Server

Do not uninstall TMMS 8.0 before backing up the data on the server. Otherwise, all data will be lost.
A. Back up TMMS 8.0 SP1.

To back up the database and configuration:

1. Download the migration tool on the computer where the TMMS 8.0 Management Server is installed.

   Example: C:\migration\migration.exe

2. Run migration.exe.
3. On the migration tool UI, go the Backup current version section.
4. Select **8.0** on the **Version** dropdown.
   The server’s installation path will appear in the **Path** field, as shown in the image below:
5. Set the backup path for the database:
   1. Log on to the computer where the database server is installed.
   2. Create a new folder in the C:\ directory. For example: C:\bak.
      This will be used as the backup path for the database file.
   3. Go back to the migration tool and input the backup path in the **Database Path** field.
   4. Click the **Backup** button.

When the backup is finished, all the configuration files will be stored in the C:\migration\bak directory. The database backup file will be stored in the path you specified in Step 5.

- The C:\migration directory is the folder of the migration tool. The bak folder is generated automatically in the same path as the migration.exe file.
- Do not change the name of the database backup file.

B. Copy the backup files to the TMMS 9.0 Patch 1 machine.

You need to copy the TMMS 8.0 backup files to the computer where TMMS 9.0 Patch 1 will be installed, so you can restore them later on.

- Database backup file

  If you will use a different SQL server for TMMS 9.0 Patch 1, you need to manually copy the backup file to the computer where the SQL server for TMMS 9.0 Patch 1 is installed.

  There is no need to manually copy the database file if you will use the same SQL server for TMMS 9.0 Patch 1.

  Trend Micro recommends using the same SQL server version for TMMS 8.0 and 9.0 Patch 1. If you use different versions, make sure that the database backup file could be restored from TMMS 8.0 to TMMS 9.0 Patch 1.

- Configuration backup files
  1. Copy the migration tool package to the computer where the TMMS 9.0 Patch 1 Management Server will be installed.
  2. Do one of the following:
     - If you will install version 9.0 Patch 1 on a different computer, get the configuration backup files from C:\migration\bak on the old machine, and copy them onto the target computer.
     - If you will install TMMS 9.0 Patch 1 on the same computer, please do not copy the configuration file. Instead, use the default settings provided by the migration tool.

7.1.3 Installing TMMS version 9.0 Patch 1

Refer to the Installation and Deployment Guide for detailed installation instructions.

TMMS versions 8.0 and 9.0 Patch 1 cannot be installed on the same computer at the same time. If you want to install version 9.0 Patch 1 on the same computer where version 8.0 is installed, you should uninstall version 8.0 and OfficeScan before installing version 9.0 Patch 1.

- If you are using the same SQL server, you need to create a new database name during the installation. Do not connect the database that you used for version 8.0.
- If you are using a different SQL server, make sure you are connected to the new server during the version 9.0 Patch 1 installation.
- If you will transfer the database/configuration to another TMMS 9.0 Patch 1 server, create a new database on the new TMMS 9.0 Patch 1 server so that the records on the current database will not be overwritten after migration.

B. Install the Blackberry tool.

Install the Blackberry tool on the machine of the Management Server 9.0 Patch 1. The installation path should be the same as the installation path of the Blackberry tool on Management Server 8.0.

If you do not use the Blackberry tool, skip this step.

C. Install the Local Communication Server.

If you will install the Local Communication Server on the same computer that hosts the TMMS 8.0 Communication Server, uninstall the TMMS 8.0 Communication Server first.

Install the Local Communication Server on a computer that has the same server address and port as the TMMS 8.0 Communication Server. This will allow TMMS 9.0 Patch 1 to recognize and manage the existing devices enrolled in TMMS 8.0.

TMMS does not support migration using a Cloud Communication Server. If you want to use a Cloud Communication Server, you will need to re-enroll all registered mobile devices.

If you are using public or private SSL certificates in version 8.0, import the SSL certificates that you exported in Pre-Migration Step C.

For the steps on installing the Local Communication Server and importing the SSL certificates, refer to "Installing the Local Communication Server" section of the TMMS 9.0 Patch 1 Installation and Deployment Guide (Chapter 3, Page 3-14).

7.1.4 Restoring the database and configuration

To restore the database and configuration on TMMS 9.0 Patch 1:

1. Run the migration tool on the computer where the TMMS 9.0 Patch 1 Management Server is installed.
2. Go to the Migrate data to destination section and select **9.0** from the **Version** dropdown. A correctly installed server will show the installation path "C:\Program Files\Trend Micro\Mobile Security" in the **Path** field.
3. In the **Database Path** field, do one the following:
   - If you are using the same SQL server, input the path where you saved the backup file.
   - If you are using a different SQL server, input the path on the target SQL server where you had copied the backup file. This was done in the Database and Configuration Backup Step B.
4. Click the **Restore** button.

   A database backup file of the TMMS 9.0 Patch 1 Management Server will be generated on the database server for exception and rollback.

After the migration, a dialog window will show the result. If the migration is successful, proceed to the next step. If the migration failed, check the logs in the migration tool directory to get detailed information, and then try to migrate again.

7.1.5 Uploading the End User License Agreement (EULA) and upgrading the devices

End User License Agreement

When the migration is finished, upload the customized End User License Agreement (EULA) manually. For the procedure, refer to the “Customizing Mobile Security Terms of Use” section of the TMMS 9.0 Patch 1 Installation and Deployment Guide (Chapter 4, Page 4-14).

Device Agents

All device agents will receive an update / upgrade notification.

Android devices will receive a notification to upgrade the agent to 9.0 Patch 1. After the upgrade, the device can be managed by the server through the new agent.

iOS devices will receive a notification to download the new iOS agent from the app store, and then an application icon named “TMMS upgrade” will be provisioned to the home screen. When the agent is installed, users need to click the icon in order for the agent to communicate with the server. The TMMS upgrade icon will be deleted automatically after the agents connect to the server. There is no need to re-enroll the device, nor to remove or re-install any profile.

7.1.6 FAQ

Q: Before doing restoration, do we need to copy any file from TMMS 8.0?

A: Yes. You need to copy the following files:

- Database backup file
- Configuration backup files

Q: Can we migrate from TMMS 8.0 using SQL Server 2008 to TMMS Mobile Device Management (MDM) 9.0 using SQL Server 2005?

A: No. Trend Micro recommends using the same version of SQL Server for TMMS 8.0 and TMMS 9.0. If you use different versions, make sure that the database backup file could be restored from TMMS 8.0 to TMMS 9.0 Patch 1.

7.2 > Backup & Restore

Download the TMMS Backup and Restore tool to do the backup and restore
http://esupport.trendmicro.com/media/13437067/Backup_and_Restore.zip
This tool only support TMMS 9.x, Versions other than TMMS 9.x are not supported.

7.2.1 Pre-Backup

The following terms will be used in this article:
Source Server (Source Management Server): The management server to back up
Target Server (Target Management Server): The management server to restore the settings

Source Database Server: The database server used by the source management server
Target Database Server: The database server used by the target management server

You may use the following tips in using the tool:
For Exchange Connector, you need to download installation package from the web console and install it after restoration.
This tool supports backup and restore between the same versions of management servers.
This tool does NOT back up the configurations of Local Communication Server (LCS). If LCS is used, it will still be used by the target management server after restoration.
After restoration, all configurations are persisted; all devices remain managed. There is no need to reenroll any device.

7.2.2 Backup Source Management server

The backup files include:

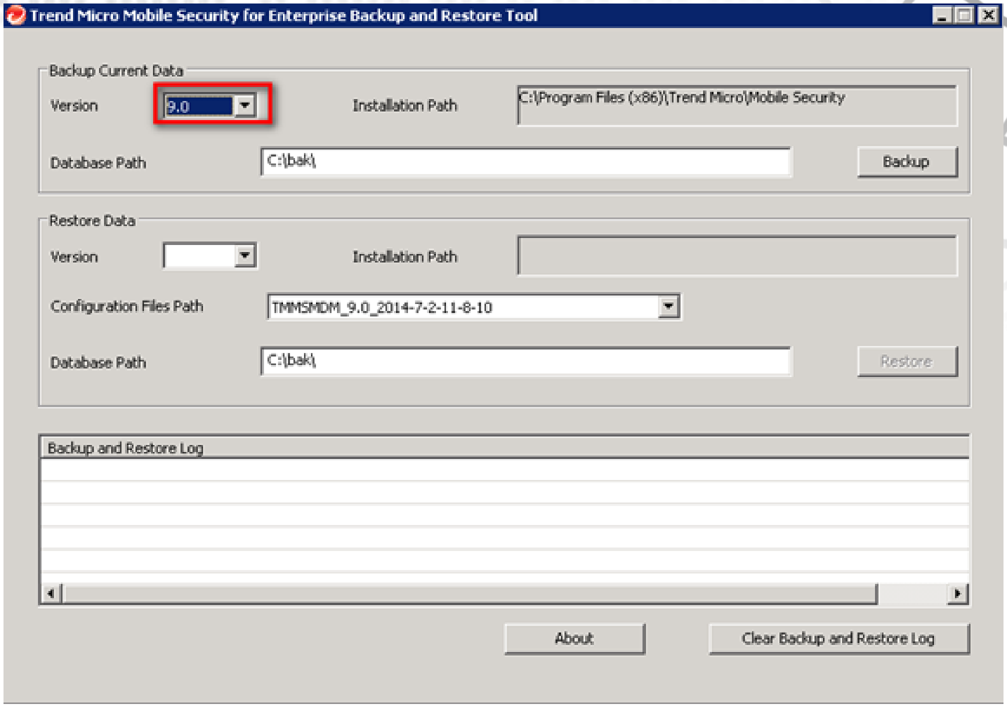
- Database backup file – This is the backup of the database used by the source management server. By default, the backup file is under the database server's c:\bak.
- Configuration backup files - These are the backup of the configuration files on the source management server. By default, the backup file is under backup & restore tool folder.

Do not uninstall the source management server before backing up the data on the server. Otherwise, all data will be lost.

Below is the steps to back up the database and configurations:

1. Copy the the TMMS Backup and Restore tool on the machine where the source management server is installed.
   Example: C:\Backup_and_Restore\Backup_and_Restore.exe
2. Run Backup_and_Restore.
3. On the tool’s UI, go to the Backup Current Data section.

4. Select 9.0 on the Version dropdown list. The installation path will automatically be shown in the Installation Path field.



Trend Micro Mobile Security for Enterprise Backup and Restore Tool

Backup Current Data

Version: 9.0

Installation Path: C:\Program Files (x86)\Trend Micro\Mobile Security

Database Path: C:\bak\

Restore Data

Version:

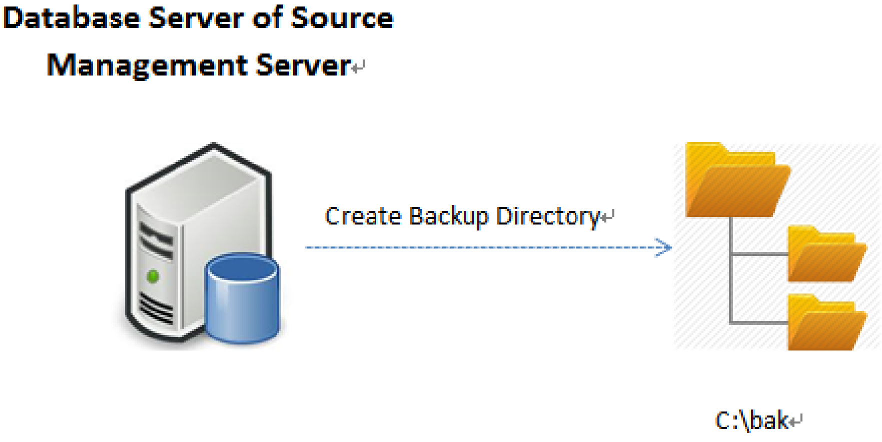
Installation Path:

Configuration Files Path: TMMSMDM_9.0_2014-7-2-11-8-10

Database Path: C:\bak\

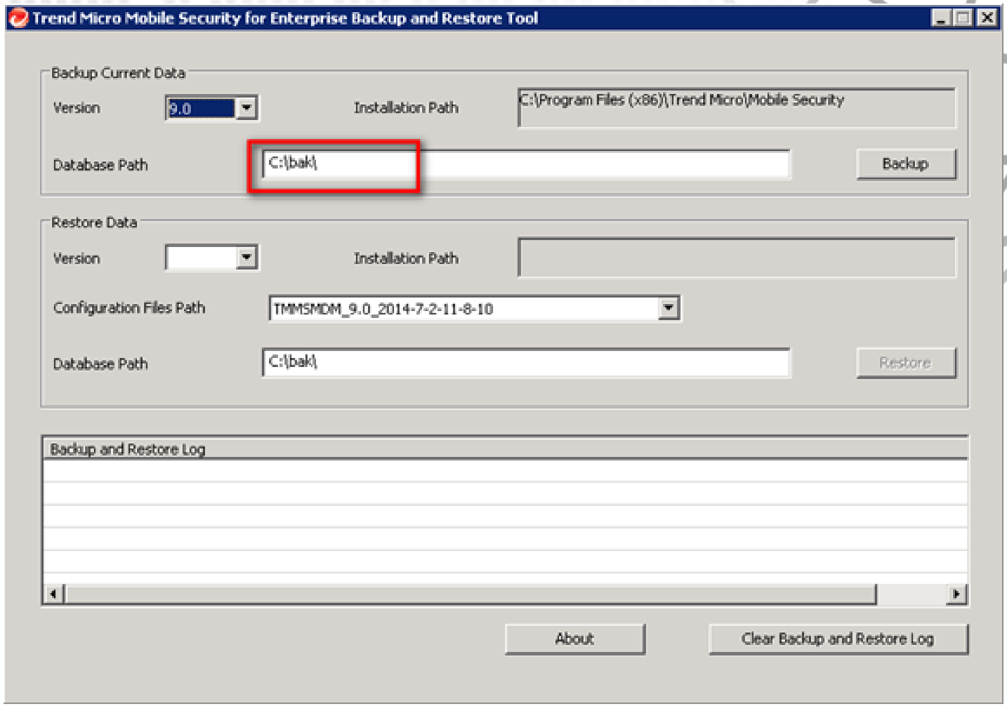
Backup and Restore Log

5. Set the backup path for the database:
    1. Log on to the machine where the database server is installed.
    2. Create a new folder for the database backup, for example, C:\bak.



This will be used as the backup path for the database file.

3. Go back to the Backup and Restore tool and enter the backup path in the Database Path field.



Trend Micro Mobile Security for Enterprise Backup and Restore Tool

Backup Current Data

Version: 9.0

Installation Path: C:\Program Files (x86)\Trend Micro\Mobile Security

Database Path: C:\bak\

Restore Data

Version:

Installation Path:

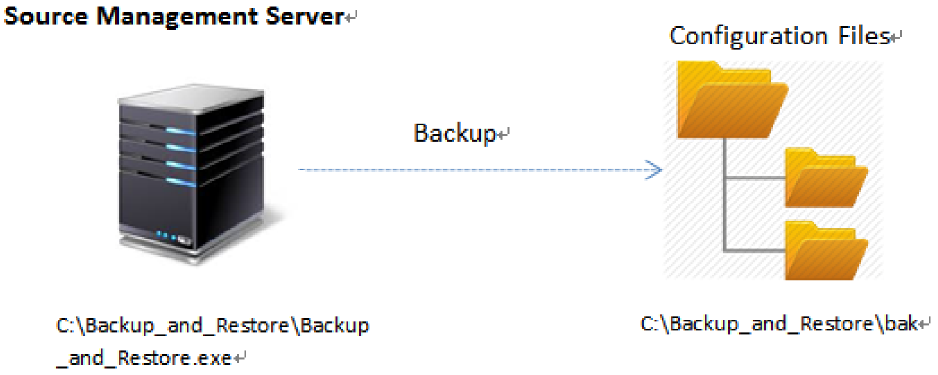
Configuration Files Path: TMMSMDM_9.0_2014-7-2-11-8-10

Database Path: C:\bak\

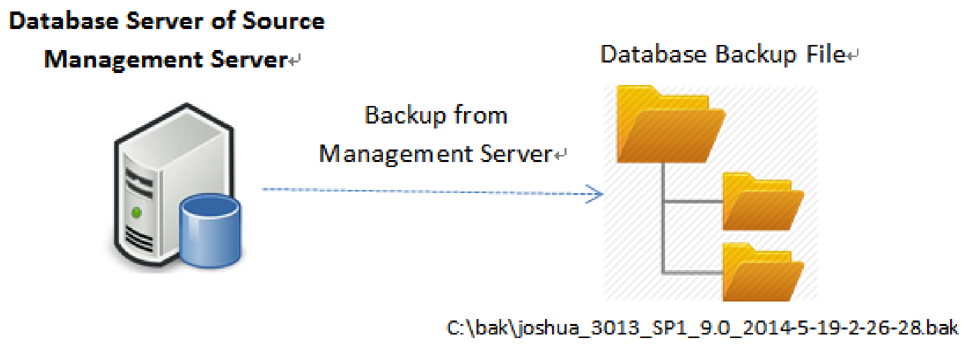
Backup and Restore Log

6. Click the **Backup** button.

When the backup is finished, all the configuration files will be stored in the [Backup_and_Restore_Tool_Folder]\bak. For example, C:\Backup_and_Restore\bak directory.



Source Management Server
Configuration Files
Backup
C:\Backup_and_Restore\Backup_and_Restore.exe
C:\Backup_and_Restore\bak


Database Server of Source Management Server
Backup from Management Server
Database Backup File
C:\bak\joshua_3013_SP1_9.0_2014-5-19-2-26-28.bak

The database backup file will be stored in the path you specified in Step 5.

- The bak folder will be created automatically in the same path as theBackup_and_Restore.exe file.
- Do not change the name of the database backup file. Otherwise, the restoration will fail.

Copy the backup files to the target management server

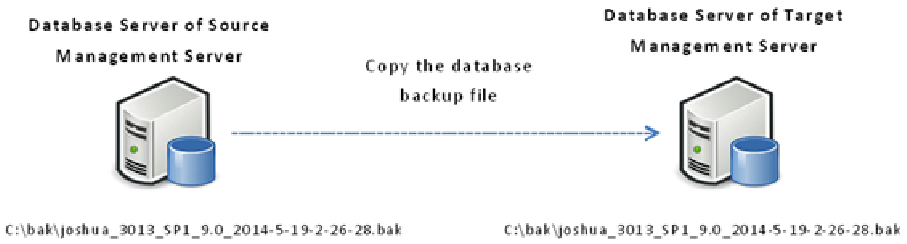
You need to copy the backup files to the machine where the target management server will be installed.

The following explains the two kinds of backup files:

Database backup files

If you use a different database server for the target management server, you need to manually copy the database backup file to the machine where the target database server is installed.

Do NOT change the filename when copying the database backup file.


Database Server of Source Management Server
Copy the database backup file
Database Server of Target Management Server
C:\bak\joshua_3013_SP1_9.0_2014-5-19-2-26-28.bak
C:\bak\joshua_3013_SP1_9.0_2014-5-19-2-26-28.bak

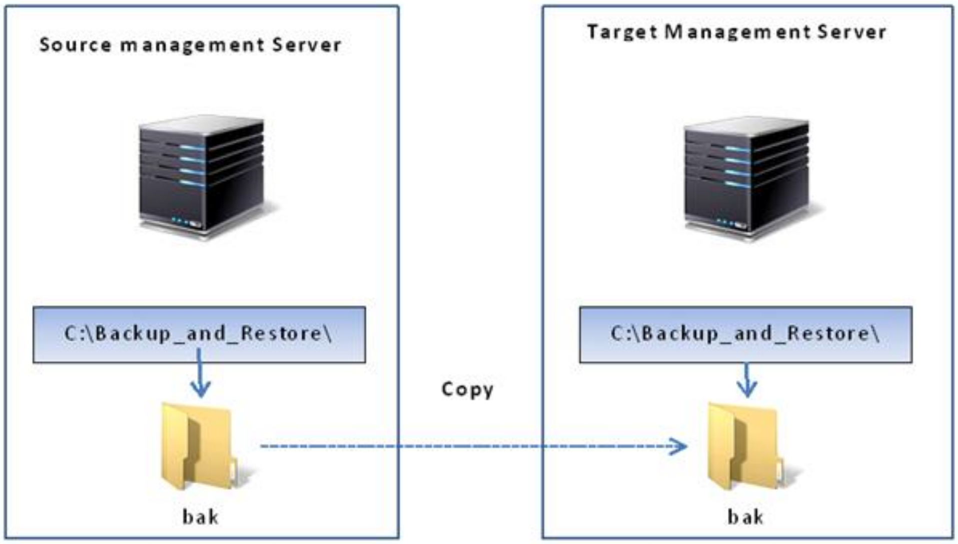
There is no need to copy the database file if you will use the same database server for the source and target management servers.

Trend Micro recommends using the same version of database server for the source and target management servers. If you use different versions, make sure that the database backup files can be restored between these two versions.

Configuration backup files

If you try to restore the old settings to the same management server (i.e. the source management server is also the target management server), there is no need to copy the configuration files. Otherwise, do the following:

1. Copy the folder containing the Backup and Restore tool to the machine where the target management server is installed.
2. Copy the folder [Backup_and_Restore_Tool_Folder]\bak (for example, C:\Backup_and_Restore\bak) from the source management server, and put it to the folder containing the tool on the target management server.



7.2.3 Install Target management server (Optional)

If the target server is not the source server, you need install the target server before doing the restoration. Refer to the Installation and Deployment Guide for detailed installation instructions.

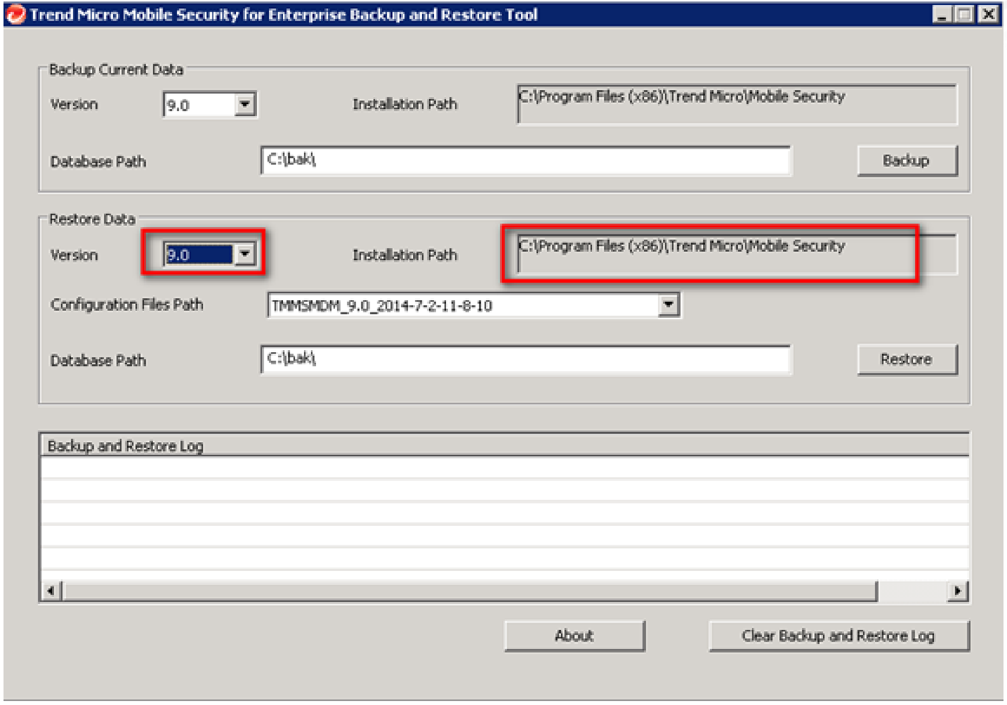
If you use the same database server for the target management server, you need to create a new database during the installation. Do not use the database used by the source server. If the target management server is not freshly installed, you need configure it to use a new database before the restoration.

7.2.4 Restore Target Server

Before restoration, make sure the source management server is stopped or uninstalled.

To restore the database and configuration:

1. Run the TMMS Backup and Restore tool on the machine where the target management server is installed.
2. Go to the Restore Data section and select **9.0** from the **Version** dropdown. The installation path will be shown in the Installation Path field.



Trend Micro Mobile Security for Enterprise Backup and Restore Tool

Backup Current Data

Version: 9.0

Installation Path: C:\Program Files (x86)\Trend Micro\Mobile Security

Database Path: C:\bak\

Restore Data

Version: 9.0

Installation Path: C:\Program Files (x86)\Trend Micro\Mobile Security

Configuration Files Path: TMMSMDM_9.0_2014-7-2-11-8-10

Database Path: C:\bak\

Backup and Restore Log

3. Select one configuration file path you have backed up. The folder name contains the timestamp.
4. In the Database Path field, do one the following:
   - If you use the same database server as the source server, enter the path where you saved the backup file.
   - If you use a different database server from the source server, enter the path on the target database server where you had copied the backup file. This was done in Database and Configuration Backup.
5. Click the **Restore** button. When the restoration is complete, the result will prompt.

If the restoration fails, check the logs in the tool folder to get detailed information.

7.2.5 Post-Restore

1. After restoration, check the Configuration and Verification page to validate the settings.
2. If the target management server is different from the source server, make sure the source management server is uninstalled or stopped after the restoration. Otherwise, both the two management servers may manage the devices at the same time.

3. Try to remote lock a device on the management web console to simply check whether the devices can be managed.

7.2.6 FAQ

Q: Before doing restoration, do we need to copy any files from the source server?
A: Yes. You need to copy the following files:

- Database backup file
- Configuration backup files

Q: Can we restore from TMMS server using SQL Server 2008 to TMMS server using SQL Server 2005?
A: No. Trend Micro recommends using the same version of database server for the source and target management servers. If you use different versions, make sure that the database backup files can be restored between the two versions.

Chapter 8: Trend Micro Knowledgebase and Contacting Support

8.1 > Knowledge base

If issues found during the recovery and isolation process continue to persist, please consult the Trend Micro

Knowledge Base or contact Technical Support.
http://esupport.trendmicro.com/en-us/business/pages/technical-support.aspx

http://esupport.trendmicro.com/en-us/business/pages/technical-support/mobile-security-for-enterprise.aspx

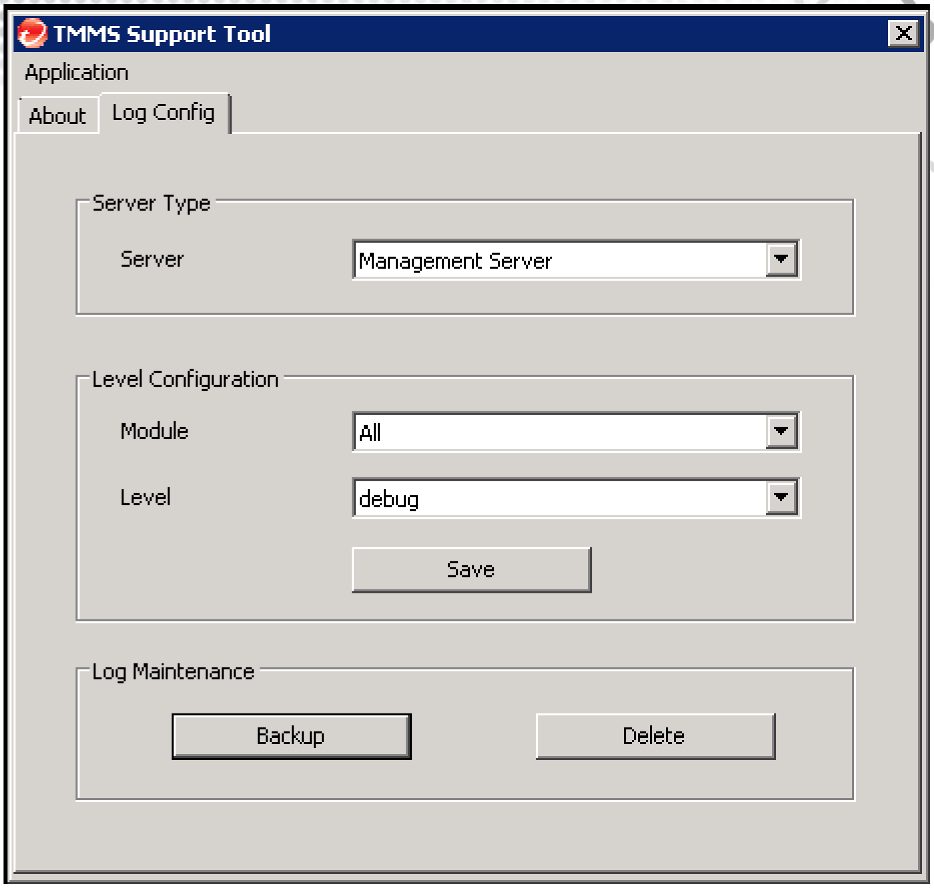
http://esupport.trendmicro.com/en-us/business/pages/about-support.aspx

8.2 > Contacting Trend Micro Support

To help Trend Micro support team provide better service, please collect following information before you contact TrendMicro, then, TrendMicro support engineer can give you meaningful update in the first reply

8.2.1 Server debug log collect

TmmsSupportTool.zip can be used for server debug log collect.
It can be download from http://esupport.trendmicro.com/media/13422640/TmmsSupportTool.zip
This support tool contains the following features:
1 Certificate configuration tool for Local Communication Server
2 Database check and configuration tool for Management Server
3 Log collection tool for Management Server and Local Communication Server



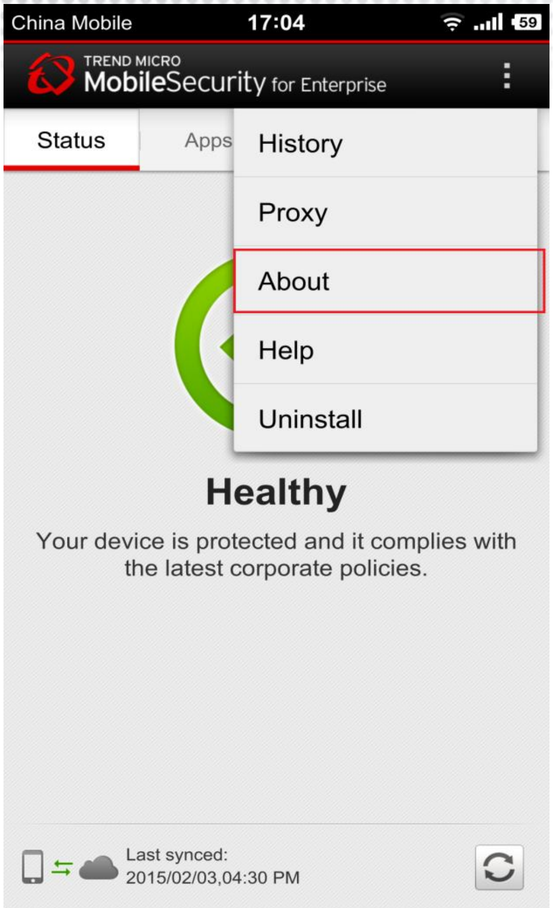
Server: Management Server

Module: All

Level: debug

8.2.2 Android debug log collect

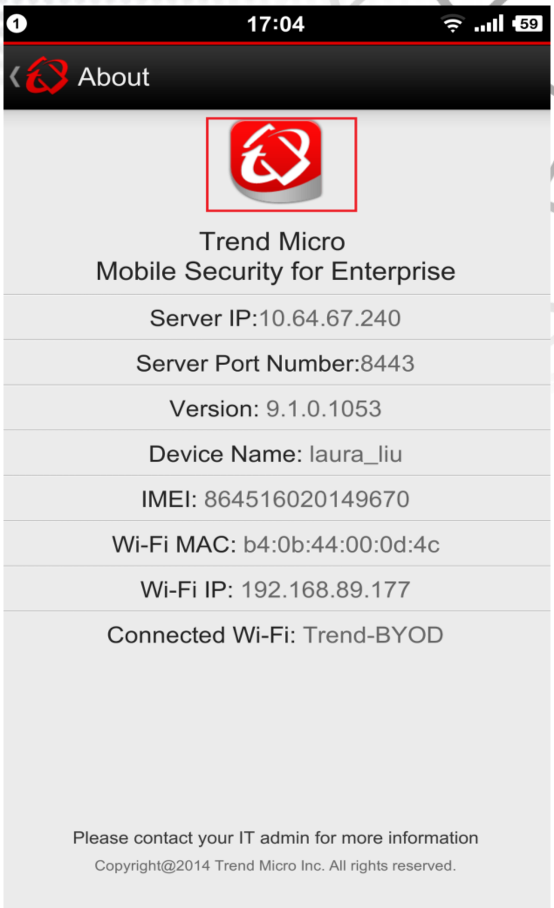
Android client can collect debug log. Open android client, find About. Click the icon 5 times, you can see the UI. Click “Start collecting Log”, then use TMMS client. After you reproduce the issues, click “Stop collecting Log”. You can get the log on SDCARD path.



Healthy

Your device is protected and it complies with the latest corporate policies.

Last synced:
2015/02/03,04:30 PM



Trend Micro
Mobile Security for Enterprise

Server IP:10.64.67.240

Server Port Number:8443

Version: 9.1.0.1053

Device Name: laura_liu

IMEI: 864516020149670

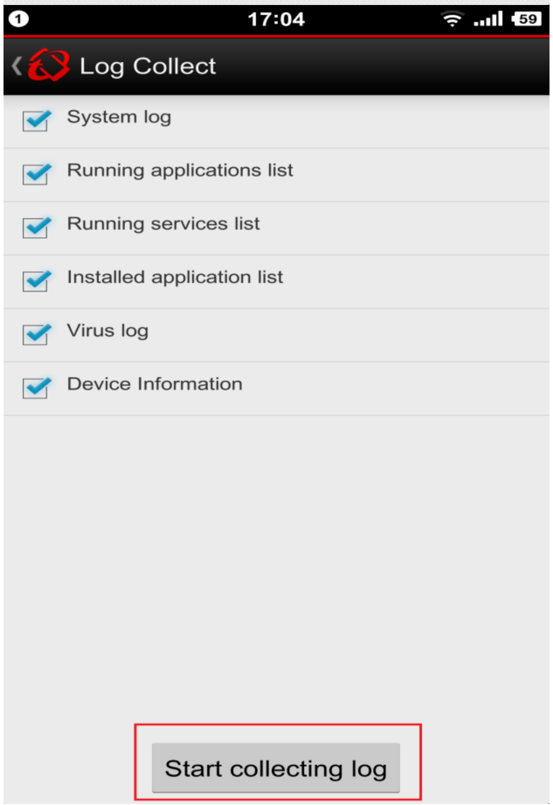
Wi-Fi MAC: b4:0b:44:00:0d:4c

Wi-Fi IP: 192.168.89.177

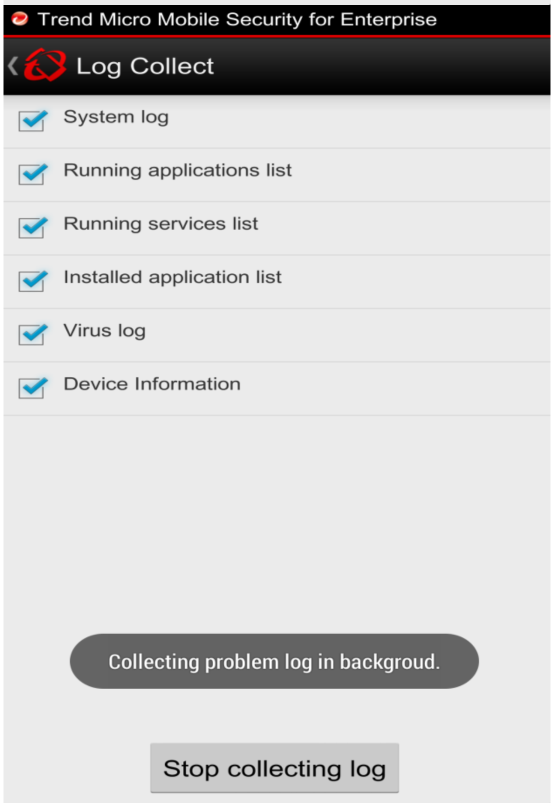
Connected Wi-Fi: Trend-BYOD

Please contact your IT admin for more information

Copyright@2014 Trend Micro Inc. All rights reserved.

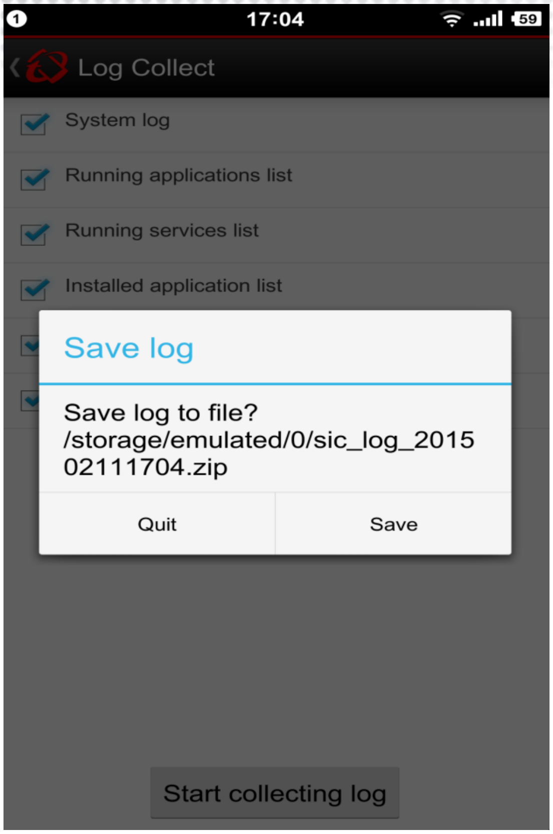


☑ System log
☑ Running applications list
☑ Running services list
☑ Installed application list
☑ Virus log
☑ Device Information



☑ System log
☑ Running applications list
☑ Running services list
☑ Installed application list
☑ Virus log
☑ Device Information

Collecting problem log in backgroud.

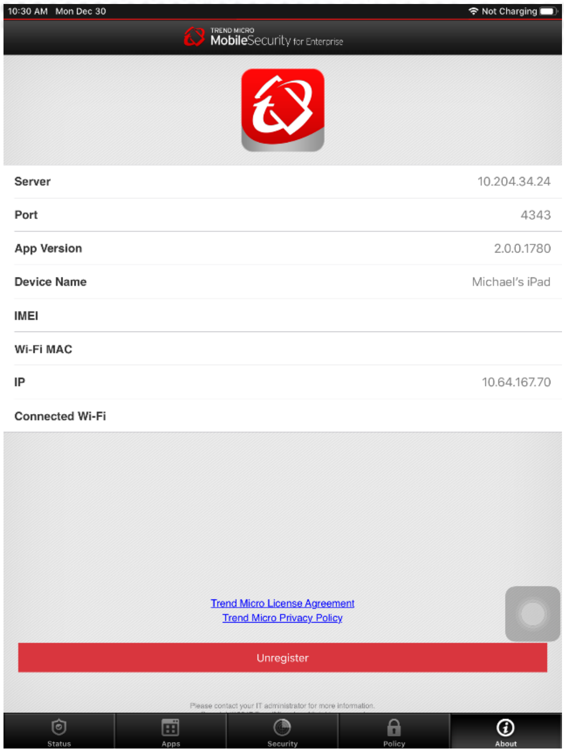


Save log

Save log to file?
/storage/emulated/0/sic_log_2015
02111704.zip

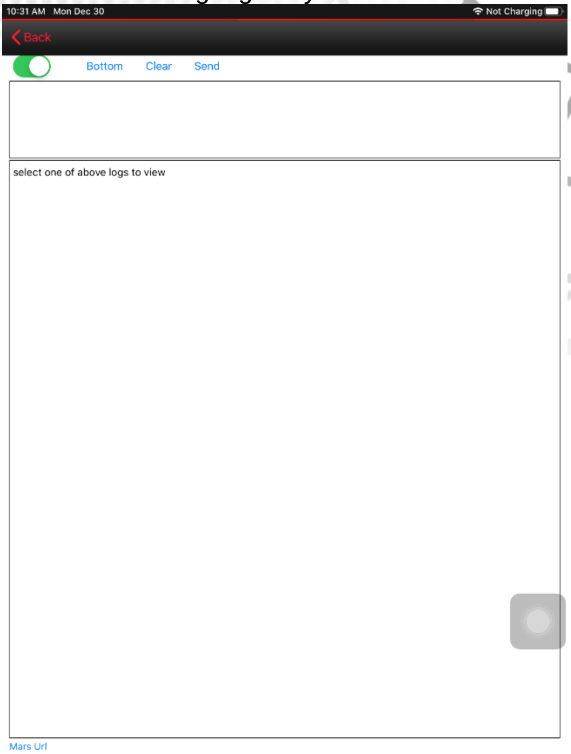
8.2.3 iOS debug log collect

iOS clients can collect debug logs. To enable an iOS client to collect debug logs, open the iOS client, tap About, and tap the agent icon five times to open the UI. Enable the debug log collecting function and then use the TMMS client. After you reproduce the issues, click the Send button to send the debug logs to your email box.click send button to send the debug logs to your mail-box.

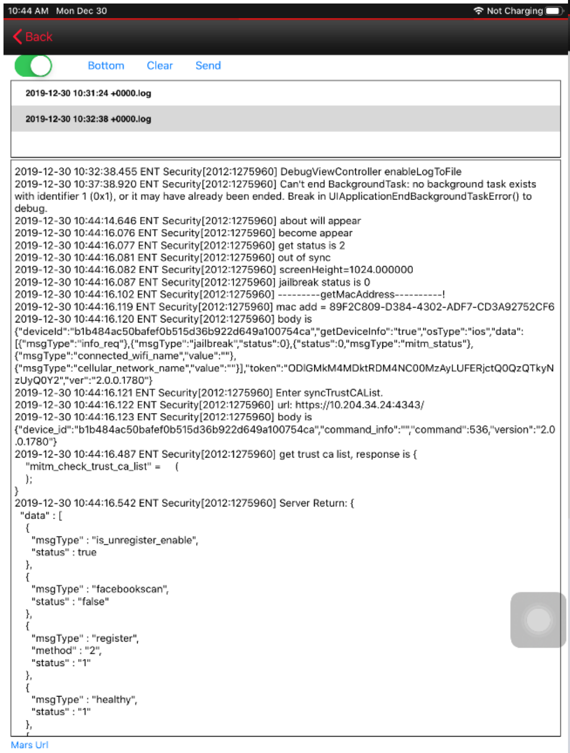

10:30 AM Mon Dec 30
Not Charging
TREND MICRO MobileSecurity for Enterprise
Trend Micro License Agreement
Trend Micro Privacy Policy
Unregister
Status
Apps
Security
Policy
About

Server	10.204.34.24
Port	4343
App Version	2.0.0.1780
Device Name	Michael's iPad
IMEI	
Wi-Fi MAC	
IP	10.64.167.70
Connected Wi-Fi	

Please contact your IT administrator for more information.



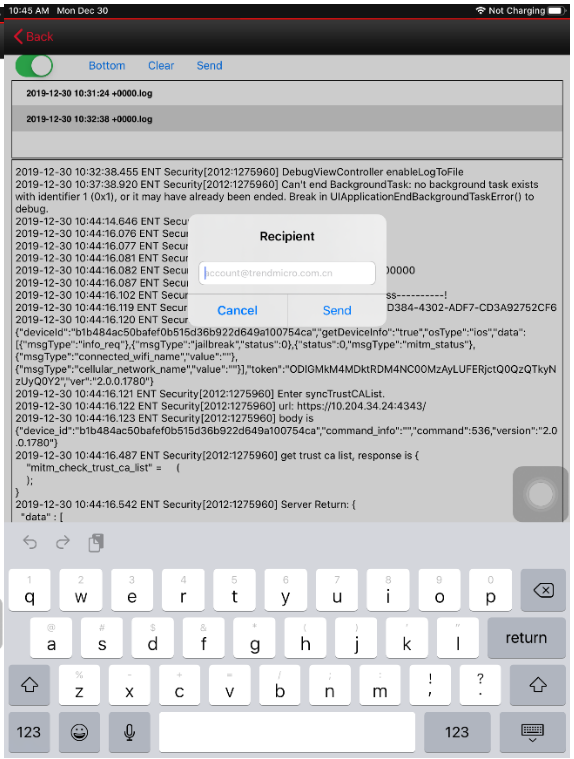
select one of above logs to view



2019-12-30 10:31:24 +0000.log

2019-12-30 10:32:38 +0000.log

```
2019-12-30 10:32:38.455 ENT Security[2012:1275960] DebugViewController enableLogToFile
2019-12-30 10:37:38.920 ENT Security[2012:1275960] Can't end BackgroundTask: no background task exists
with identifier 1 (0x1), or it may have already been ended. Break in UIApplicationEndBackgroundTaskError() to
debug.
2019-12-30 10:44:14.646 ENT Security[2012:1275960] about will appear
2019-12-30 10:44:16.076 ENT Security[2012:1275960] become appear
2019-12-30 10:44:16.077 ENT Security[2012:1275960] get status is 2
2019-12-30 10:44:16.081 ENT Security[2012:1275960] out of sync
2019-12-30 10:44:16.082 ENT Security[2012:1275960] screenHeight=1024.000000
2019-12-30 10:44:16.087 ENT Security[2012:1275960] jailbreak status is 0
2019-12-30 10:44:16.102 ENT Security[2012:1275960] ---------getMacAddress----------!
2019-12-30 10:44:16.119 ENT Security[2012:1275960] mac add = 89F2C809-D384-4302-ADF7-CD3A92752CF6
2019-12-30 10:44:16.120 ENT Security[2012:1275960] body is
{"deviceId":"b1b484ac50bafef0b515d36b922d649a100754ca","getDeviceInfo":"true","osType":"ios","data":
[{"msgType":"info_req"},{"msgType":"jailbreak","status":0},{"status":0,"msgType":"mitm_status"},
{"msgType":"connected_wifi_name","value":""},
{"msgType":"cellular_network_name","value":""}],"token":"ODlGMkM4MDktRDM4NC00MzAyLUFERjctQ0QzQTkyN
zUyQ0Y2","ver":"2.0.0.1780"}
2019-12-30 10:44:16.121 ENT Security[2012:1275960] Enter syncTrustCAList.
2019-12-30 10:44:16.122 ENT Security[2012:1275960] url: https://10.204.34.24:4343/
2019-12-30 10:44:16.123 ENT Security[2012:1275960] body is
{"device_id":"b1b484ac50bafef0b515d36b922d649a100754ca","command_info":"","command":536,"version":"2.0
.0.1780"}
2019-12-30 10:44:16.487 ENT Security[2012:1275960] get trust ca list, response is {
   "mitm_check_trust_ca_list" =     (
   );
}
2019-12-30 10:44:16.542 ENT Security[2012:1275960] Server Return: {
  "data" : [
   {
    "msgType" : "is_unregister_enable",
    "status" : true
   },
   {
    "msgType" : "facebookscan",
    "status" : "false"
   },
   {
    "msgType" : "register",
    "method" : "2",
    "status" : "1"
   },
   {
    "msgType" : "healthy",
    "status" : "1"
   },
```



2019-12-30 10:31:24 +0000.log

2019-12-30 10:32:38 +0000.log

```
2019-12-30 10:32:38.455 ENT Security[2012:1275960] DebugViewController enableLogToFile
2019-12-30 10:37:38.920 ENT Security[2012:1275960] Can't end BackgroundTask: no background task exists
with identifier 1 (0x1), or it may have already been ended. Break in UIApplicationEndBackgroundTaskError() to
debug.
2019-12-30 10:44:14.646 ENT Secu
2019-12-30 10:44:16.076 ENT Secur
2019-12-30 10:44:16.077 ENT Secur
2019-12-30 10:44:16.081 ENT Secur
2019-12-30 10:44:16.082 ENT Secur                                    00000
2019-12-30 10:44:16.087 ENT Secur
2019-12-30 10:44:16.102 ENT Secur                                    ss----------!
2019-12-30 10:44:16.119 ENT Secur                                    D384-4302-ADF7-CD3A92752CF6
2019-12-30 10:44:16.120 ENT Secur
{"deviceId":"b1b484ac50bafef0b515d36b922d649a100754ca","getDeviceInfo":"true","osType":"ios","data":
[{"msgType":"info_req"},{"msgType":"jailbreak","status":0},{"status":0,"msgType":"mitm_status"},
{"msgType":"connected_wifi_name","value":""},
{"msgType":"cellular_network_name","value":""}],"token":"ODlGMkM4MDktRDM4NC00MzAyLUFERjctQ0QzQTkyN
zUyQ0Y2","ver":"2.0.0.1780"}
2019-12-30 10:44:16.121 ENT Security[2012:1275960] Enter syncTrustCAList.
2019-12-30 10:44:16.122 ENT Security[2012:1275960] url: https://10.204.34.24:4343/
2019-12-30 10:44:16.123 ENT Security[2012:1275960] body is
{"device_id":"b1b484ac50bafef0b515d36b922d649a100754ca","command_info":"","command":536,"version":"2.0
.0.1780"}
2019-12-30 10:44:16.487 ENT Security[2012:1275960] get trust ca list, response is {
   "mitm_check_trust_ca_list" =     (
   );
}
2019-12-30 10:44:16.542 ENT Security[2012:1275960] Server Return: {
  "data" : [
```

Chapter 9: Miscellaneous

9.1 > Changing Web Console Timeout Period

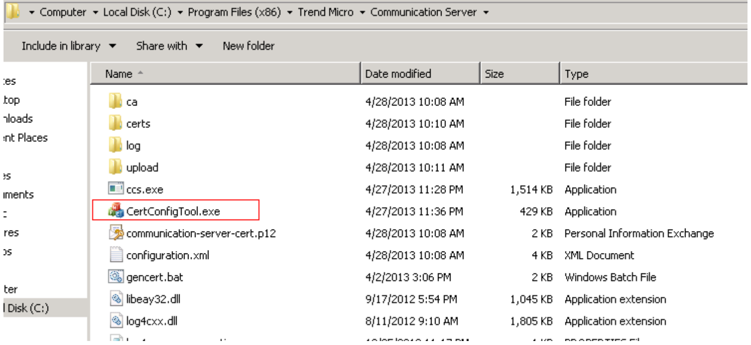
1. Open the TmOMSM.ini from...\Trend Micro\Mobile Security\
2. Modify the 'SessionTimeout' value; the default value is 900 seconds.
3. Save

Note: The minimum value is "60", if the value is set lower than "60" it will be "60"

9.2 > Changing LCS Certificate

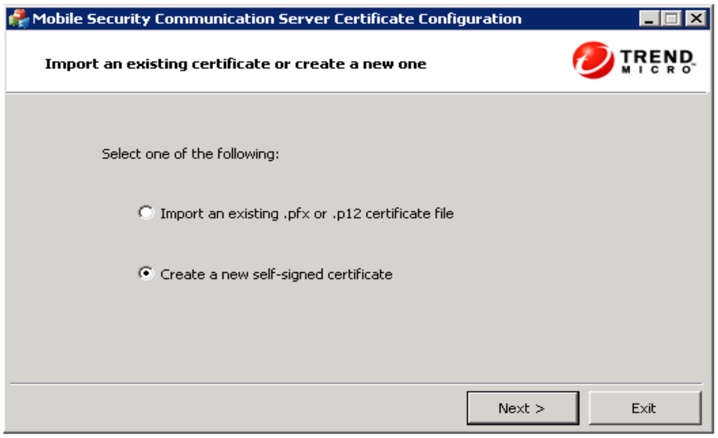
Changing SSL certificate for local communication server

1. Logon to the computer that LCS installed. Double click **CertconfigTool.exe**



Name	Date modified	Size	Type
ca	4/28/2013 10:08 AM		File folder
certs	4/28/2013 10:10 AM		File folder
log	4/28/2013 10:08 AM		File folder
upload	4/28/2013 10:11 AM		File folder
ccs.exe	4/27/2013 11:28 PM	1,514 KB	Application
CertConfigTool.exe	4/27/2013 11:36 PM	429 KB	Application
communication-server-cert.p12	4/28/2013 10:08 AM	2 KB	Personal Information Exchange
configuration.xml	4/28/2013 10:08 AM	4 KB	XML Document
gencert.bat	4/2/2013 3:06 PM	2 KB	Windows Batch File
libeay32.dll	9/17/2012 5:54 PM	1,045 KB	Application extension
log4cxx.dll	8/11/2012 9:10 AM	1,805 KB	Application extension

2. If you want to regenerate a new self-signed certificate, select "**Create a new self-signed certificate**"; if you want to import existing certificates, select "**Import an existing .pfx or .p12 certificate file**". Then click **next**.



Mobile Security Communication Server Certificate Configuration

Import an existing certificate or create a new one

Select one of the following:

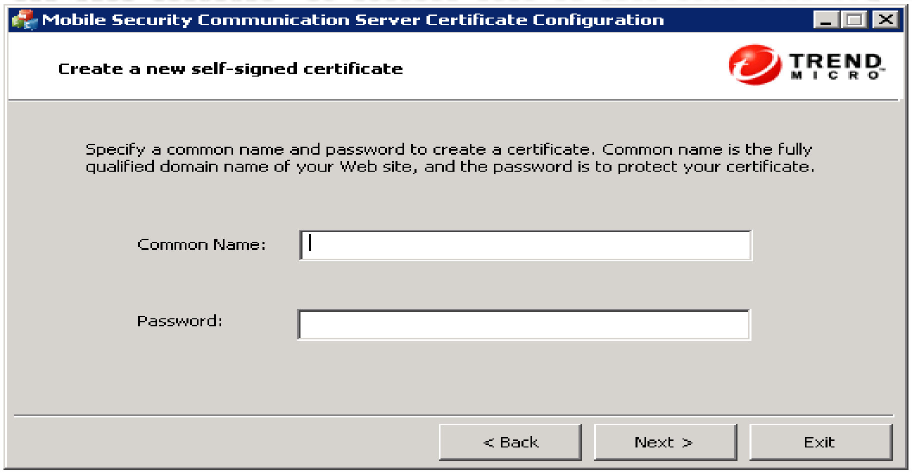
○ Import an existing .pfx or .p12 certificate file

● Create a new self-signed certificate

3. Enter required information according to your choice (regenerate a new certificate or import an existing certificate).

- Regenerate a new certificate

Input the IP address or public domain name as the **common name**, enter the password, and click **next**.



Mobile Security Communication Server Certificate Configuration

Create a new self-signed certificate

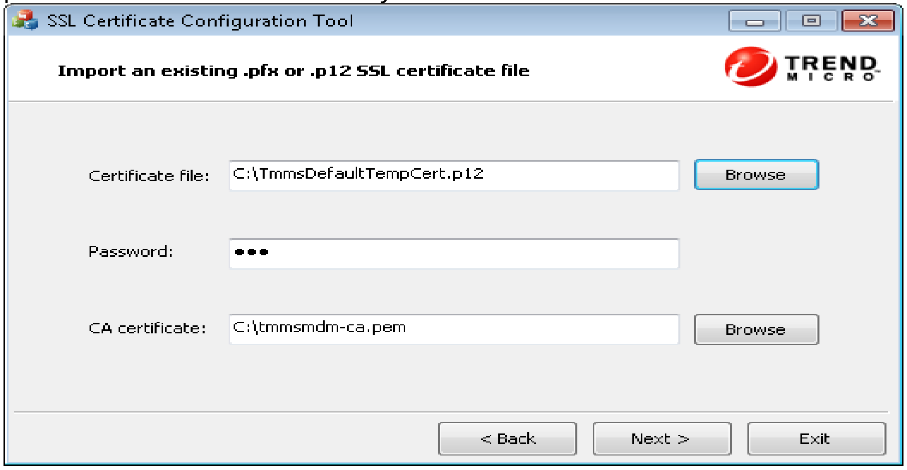
Specify a common name and password to create a certificate. Common name is the fully qualified domain name of your Web site, and the password is to protect your certificate.

Common Name:

Password:

- Import an existing certificate

Select the certificate files (.p12 or .pfx) and enter the password; and select the CA certificate file (.cer, .crt, .pem, or .der) if the certificate is self-signed, or you can leave it empty if it is issued by a public trusted certificate authority. Click “**Next**”.



SSL Certificate Configuration Tool

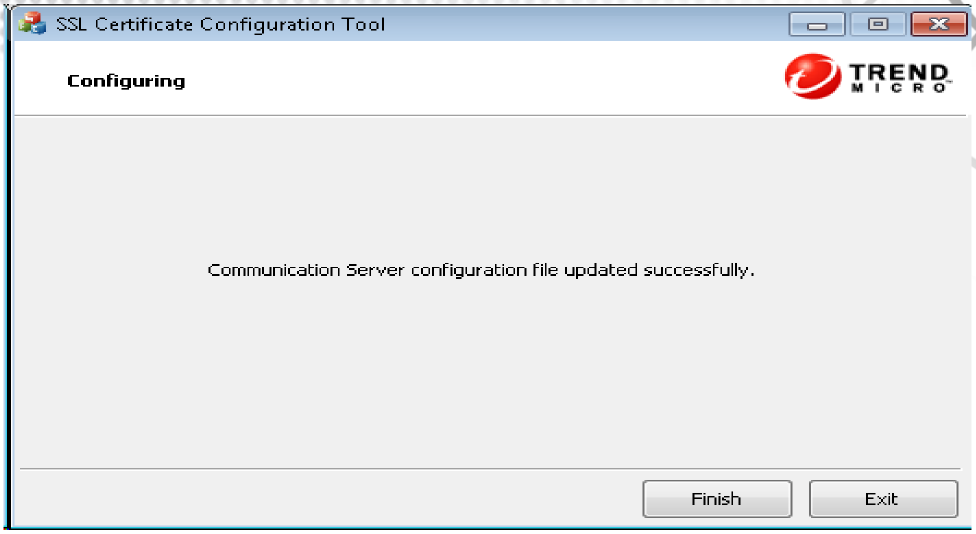
Import an existing .pfx or .p12 SSL certificate file

Certificate file: C:\TmmsDefaultTempCert.p12

Password: ●●●

CA certificate: C:\tmmsmdm-ca.pem

4. Click **Finish**.



SSL Certificate Configuration Tool

Configuring

Communication Server configuration file updated successfully.

5. In windows services, restart **Mobile Security Communication Server** service.

9.3 > Renewing APNS Certificate

You need to renew your APNs certificate before it is expired to continue managing iOS mobile devices. Refer to the following URL for the detailed procedure:

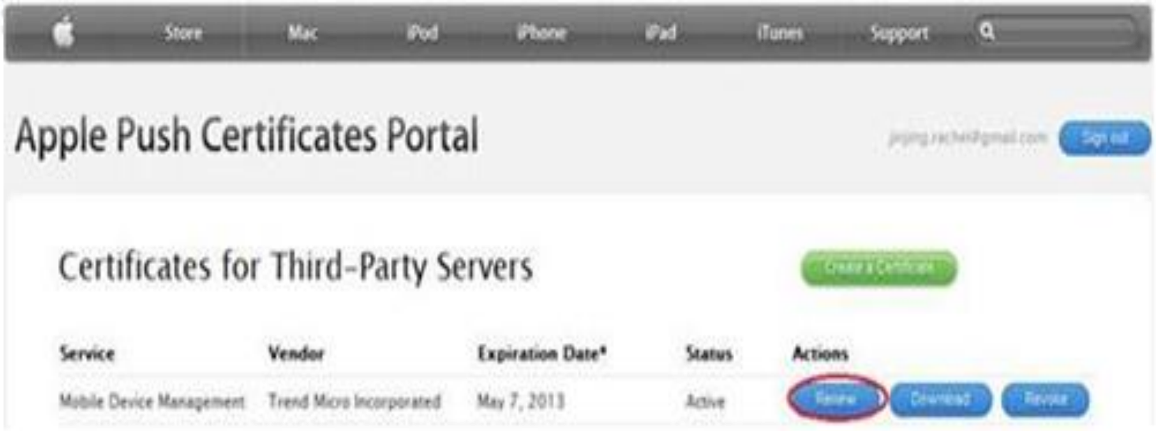
1. Create a new Certificate Signing Request (CSR).

2. Open the Trend Micro APNs Certificate Signing Portal.

- Fill in the required fields.
- Enter your TMMS Activation Code.
- Copy and paste your CSR.
- Read and accept the Trend Micro License Agreement and Submit. After you have successfully submitted the above information, you will be prompted to download the signed CSR and will get a notification about receiving an email with the signed CSR attached.

3. Open the Apple Push Certificates Portal click ‘Renew’ and upload the signed CSR (CertSigningRequest)

Note: If you click “Create a Certificate”, it will generate a new APNs certificate. Then you will need to enroll all iOS mobile device again to the Mobile Security server.



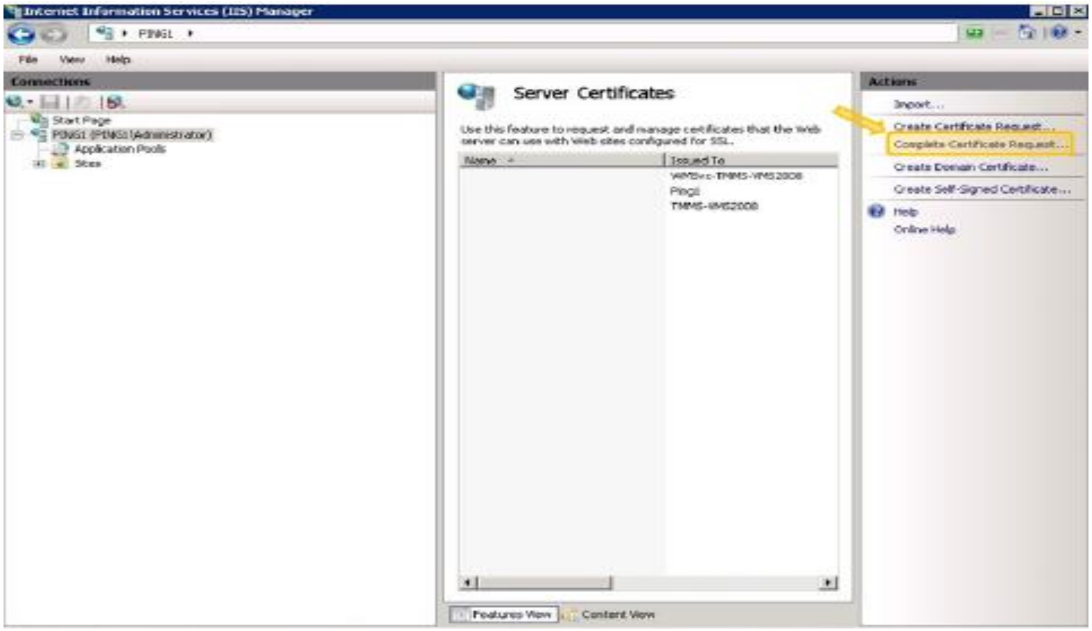
Apple Push Certificates Portal

Certificates for Third-Party Servers

Service	Vendor	Expiration Date*	Status	Actions
Mobile Device Management	Trend Micro Incorporated	May 7, 2013	Active	Renew Download Revoke

4. Download the certificate signed by Trend and Apple (.PEM) from the Apple Portal and complete the Certificate Request from the IIS

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



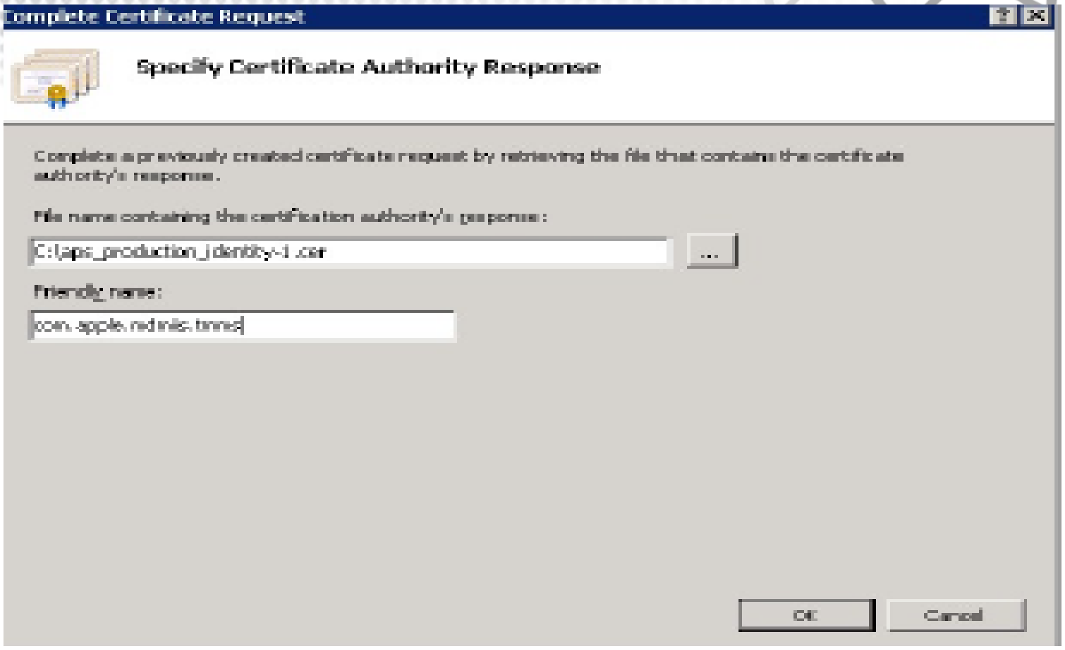
Internet Information Services (IIS) Manager
PING1
File
View
Help
Connections
Start Page
PING1 (PING1\Administrator)
Application Pools
Sites
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help
Features View
Content View

Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To
	WMSvc-TMMS-VMS2008
	Ping1
	TMMS-VMS2008

5. Select the **.cer** certificate file that you downloaded from the Apple Portal, and type Trend Micro
Note: You must manually change the **.pem** file extension to **.cer**



Complete Certificate Request

Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response:

C:\aps_production_identity-1.cer

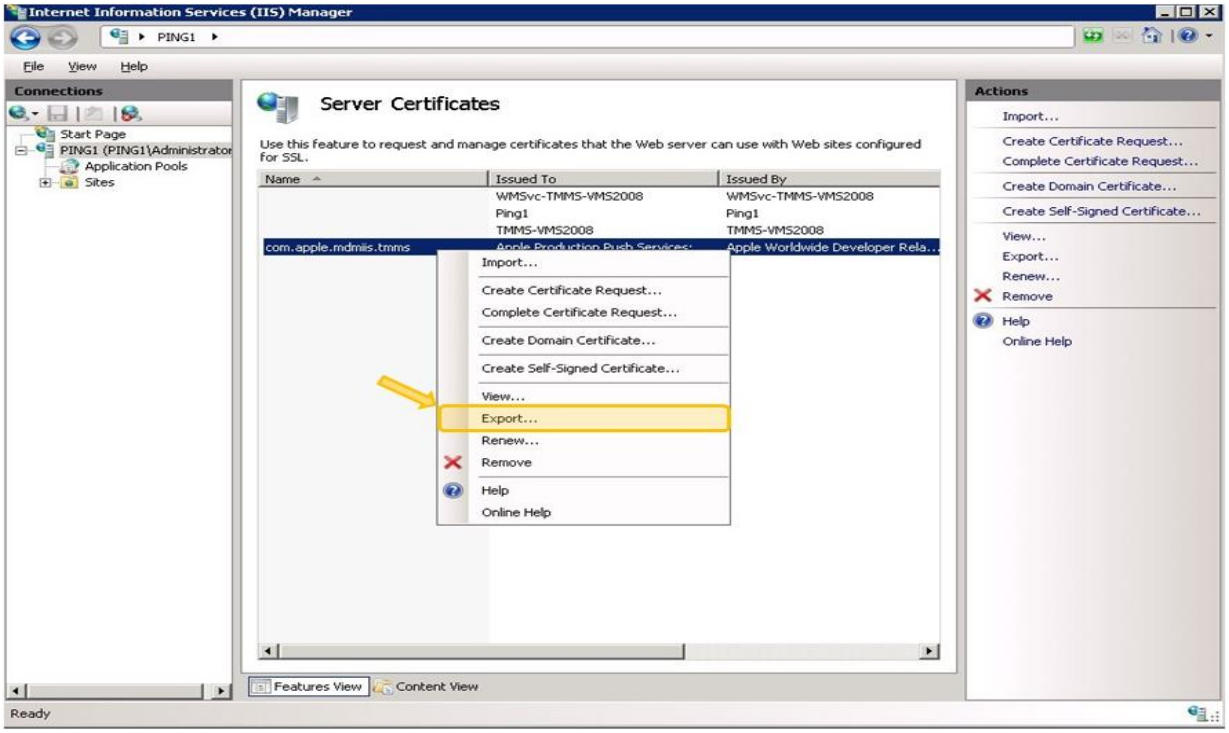
Friendly name:

com.apple.mdmiis.tmms

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

6. Select OK. The certificate will be installed on the server.
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.

7. Right-click on the certificate in the **Server Certificates** list, and then click **Export.**



Internet Information Services (IIS) Manager

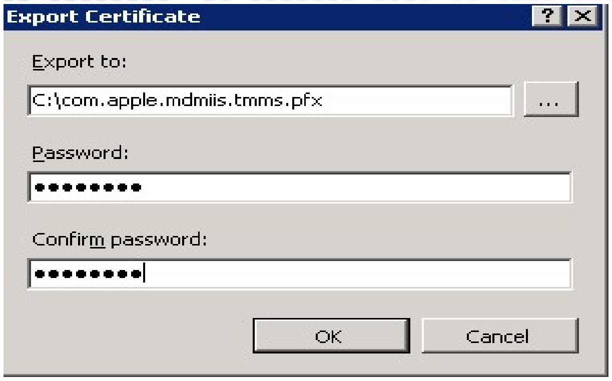
Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By
	WMSvc-TMMS-VMS2008	WMSvc-TMMS-VMS2008
	Ping1	Ping1
	TMMS-VMS2008	TMMS-VMS2008
com.apple.mdmiis.tmms	Apple Production Push Services:	Apple Worldwide Developer Rela...

PING1
File
View
Help
Connections
Start Page
PING1 (PING1\Administrator
Application Pools
Sites
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Renew...
Remove
Help
Online Help
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Renew...
Remove
Help
Online Help
Features View
Content View
Ready

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



Export Certificate

Export to: C:\com.apple.mdmiis.tmms.pfx

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

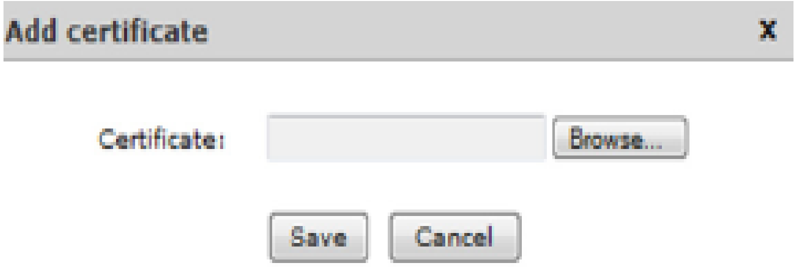
Specifying password for the certificate

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.
- 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.

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.
10. Logon to the MDM Console
Click **Administration** > **Certificate Management**, click **Add**, browse the APNs certificate (**.pfx** format) with password, the click Save.



Add certificate

Certificate:

Click **Administration** > **Communication Server Settings**, click **iOS Settings** tab, and then select the Apple Push Notification Server certificate you uploaded from the Certificate Management > click **Save**

9.4 > Troubleshooting Guide

This section provides tips for dealing with issues you may encounter when using Mobile Security.
• **User cannot input nanoscale passwords on their devices.**

Mobile device keypads can only support a certain set of characters. Mobile Security recommends that the administrator compile a list of characters supported by the devices. After compiling the list of supported characters, the administrator can then set the uninstall protection password from the management console using the list of supported characters.

- **After cancelling the Communication Server uninstallation process, the Communication Server fails to function normally.**

If the uninstallation process started deleting the files and services that are important for the Communication Server's normal operation before the process was stopped, the Communication Server may not function normally. To resolve this issue, install and configure the Communication Server again.

- **iOS mobile devices cannot enroll successfully to the Management Server, and displays "Unsupported URL" error message.**

This may happen if the system clock of SCEP server is set to the incorrect time or the Simple Certificate Enrollment Protocol (SCEP) certificate is not obtained by Trend Micro Mobile Security. Make sure that the system clock of SCEP server is set to the correct time. If the issue persists, perform the following steps:

1. Log on to the Mobile Security Administration Web console.
2. Click Administration > Communication Server Settings.
3. Without changing the settings, click Save.

- **Unable to save database Settings if you use SQL Server Express.**

If you are using SQL Server Express, use the following format in the Server address field: <SQL Server Express IP address>\sqlexpress.
Note: Replace <SQL Server Express IP address> with the IP address of SQL Server Express.

- **Unable to export the client device list in Device Management.**

This may occur if the downloading of encrypted files is disabled in the Internet Explorer. Perform the following steps to enable the encrypted files download:

1. On your Internet Explorer, go to Tools > Internet options, and then clicks the Advanced tab on the Internet Options window.
2. Under Security section, clear do not save encrypted pages to disk.
3. Click OK.

- **The status of certain Android mobile device is always Out of Sync.**

This is because the Mobile Security device administrator is not activated on that mobile device. If the user not activates Mobile Security in the Device administrators list, then the Mobile security cannot synchronize server policies with the mobile device, and displays its status as Out of Sync.

- **The content on the Policy pop-up window does not display and is blocked by Internet Explorer.**

This happens if your Internet Explorer is configured to use a .pac automatic configuration file. In that case, the Internet Explorer will block the access to a secure Web site that contains multiple frames. To resolve this issue, add the Mobile security server address to the trusted sites security zone in the Internet Explorer. To do this, perform the following steps:

1. Start Internet Explorer.
2. Go to Tools > Internet options.
3. On the Security tab, click Trusted Sites, and then click Sites.
4. In the Add this Web site to the zone test field, type the Mobile Security server URL and then click Add.

5. Click OK.