## Contents

1  Introduction ..............................................................................................................................................2

1.1  Requirements ..........................................................................................................................................2

1.2  Architecture ...........................................................................................................................................2

1.3  Feature List ............................................................................................................................................3

  1.3.1 Auto grouping for devices ..............................................................................................................3

  1.3.2 Other MobileIron Compliance Policy and actions .........................................................................3

1.4  Basic Deployment ..................................................................................................................................4

  1.4.1 TMMS Server Setting ......................................................................................................................4

  1.4.2 Deploy Android agent ....................................................................................................................6

  1.4.3 Deploy IOS agent ..........................................................................................................................9
1 Introduction

1.1 Requirements

The following requirements/conditions should be met before proceeding:

- Mobile Security for Enterprise 9.7 Patch2 version or later
- The communication server is configured to either Local Communication server or Cloud Communication Server.
- MobileIron V2 9.1.1.0
- MobileIron Admin account

1.2 Architecture

- MARS
  Mobile App Reputation is a cloud-based technology that automatically identifies mobile threats based on app behavior, crawl & collect huge number of Android apps from various Android Markets, identifies existing and brand new mobile malware, identifies apps that may abuse privacy / device resources, World's first automatic mobile app evaluation service
- SPN
  The Trend Micro Smart Protection Network delivers proactive global threat intelligence against zero-hour threats to ensure that you are always protected. We use our up-to-the-second threat intelligence to immediately stamp out attacks before they can harm you. Powering all of our products and services.
1.3 Feature List

1.3.1 Auto grouping for devices

Three TMMS labels (Dangerous, Risky, and No_TMMS) will be created along with three device customer attributes values. TMMS changes the device customer attributes' value, and then the device will be added to the labels automatically.

1.3.2 Other MobileIron Compliance Policy and actions

The administrator can set MobileIron Policy to Labels while the device has label PREDEFINED_Dangerous. There are many policies provided by MobileIron.
1.4 Basic Deployment

1.4.1 TMMS Server Setting

1. Log on to the Mobile Security administration web console.
2. Go to Administration > Communication Server Settings, and make sure the Communication Server settings are configured. If the settings are not configured, refer to the topic Configuring Communication Server Settings in the Installation and Deployment Guide for the configuration steps.
3. Click Administration > Deployment Settings.
4. Under the Server section, select Security Scan, and then select MobileIron as the MDM Solution from the drop-down list.
5. Under Register Service, configure the following AirWatch settings:
   - API URL
   - API KEY
   - Account Name
   - Password

6. Click Verify Settings to make sure Mobile Security can connect to the MobileIron server.

7. Under Data Synchronization Settings section, configure the following:
   - Security Category Prefix
1.4.2 Deploy Android agent

TMMS has two Android agent version. The MobileIron Administrator need to choose one of the following versions:

<table>
<thead>
<tr>
<th>Version</th>
<th>Pros and Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google play version</td>
<td>Administrator will need to send an email to the end-user with QR code or Enrollment Key. End-users need to open TMMS agent and scan the QR code or manually enter the Enrollment Key to register their device to server. Agent can be updated automatically.</td>
</tr>
<tr>
<td>TMMS server version</td>
<td>Administrator need to send an email to end-user ask them to launch TMMS Agent, after end-user launch TMMS Agent, TMMS agent will register to TMMS server. While TMMS agent has new version, end-user need to type the upgrade button in the notification bar.</td>
</tr>
</tbody>
</table>

Google Play build

1. Login to the MobileIron console, then go to Apps > App Catalog.
2. Click **Google Play**, search for "ent security", then select **Mobile Security for Enterprise**.

![](image1.png)

3. Keep the default application names.

4. Tick **Feature this App in the Apps@Works catalog**, then click **Next**.

5. Keep the APP VPN Settings and APP Settings to default, then click **Next**.

6. Click **Finish**.

**Local Server build**

1. Login to the TMMS web console, then go to **Administration > Deployment Settings > Android Agent**.

2. Select **Download from TMMS Server**, tick **Auto Enrollment**, and then click **Save**.

![](image2.png)
3. Go to Administration > Device Enrollment Settings > Authentication.

4. Select Authenticate using Enrollment key, tick use preset Enrollment Key, and then click Generate.

5. Uncheck the Enrollment key expires after option, the click Save.
1.4.3 Deploy IOS agent

1. Login to the MobileIron console, then go to Apps > App Catalog.

2. Click iTunes, search for "ent security", then select Mobile Security for Enterprise.

7. Keep the default application names.

8. Tick Feature this App in the Apps@Works catalog, then click Next.

9. Keep the APP VPN Settings and APP Settings to default, then click Next.

10. Click Finish.
11. Login to the TMMS Admin console and go to **Administration > Deployment Settings > iOS Agent**, then click **Download** to get the agent configuration file.

12. Login to the MobileIron admin console, then go to **Policies & Configurations**.

13. Go to **Add New > iOS and OS X > Managed App Config**, to open the iOS Managed App Config settings page.

14. Enter the name, description, TMMS agent bundle ID, and select the configuration file downloaded from Step 2: Configure TMMS for the integration.

15. Select the newly created configuration, then click **More Actions > Apply to Label** to assign the configuration to the labels.
16. Tick the name of the device(s) where the TMMS agent will be installed, then click **Apply**. A notification will appear on the selected device(s).

17. From the notification, click **Install**. The agent will be installed on the device, and will be enrolled to the TMMS Server.