

## 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

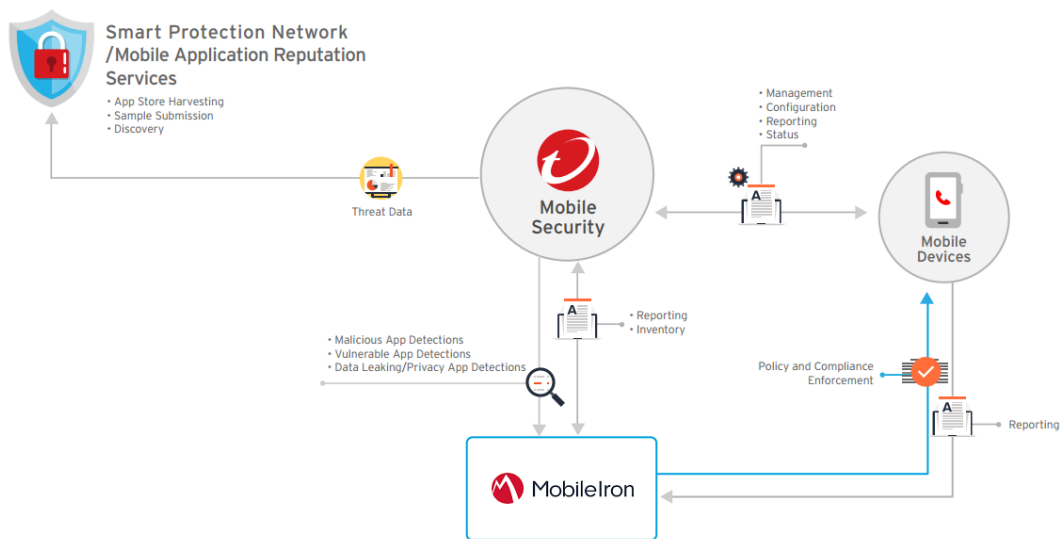
# 1 Introduction

## 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**.


> CORE

[Dashboard](#)
[Devices & Users](#)
[Admin](#)
[Apps](#)
[Policies & Configs](#)
[Services](#)
[Settings](#)
[Logs](#)


[Devices](#)
[Users](#)
[Labels](#)
[ActiveSync](#)
[Apple DEP](#)

Actions
Add Label

	NAME	DESCRIPTION	TYPE	CRITERIA
	andrew_tmms__dangerous		Filter	"common.retired" = false AND "custom.device.andrew_tmms__tmms_security_"=3
	andrew_tmms__NO_TMMS		Filter	"common.retired" = false AND "custom.device.andrew_tmms__NO_TMMS_"=1
	andrew_tmms__riksy		Filter	"common.retired" = false AND "custom.device.andrew_tmms__tmms_security_"=2

### 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.

 > CORE

[Dashboard](#)
[Devices & Users](#)
[Admin](#)
[Apps](#)
[Policies & Configs](#)
[Services](#)
[Settings](#)
[Logs](#)

[Configurations](#)
[Policies](#)
[ActiveSync Policies](#)
[Compliance Actions](#)

[Delete](#)
[More Actions](#)
[Add New](#)
 Labels: 
 Search by User 
 Policy Type: 
 Search by Name

<input type="checkbox"/>	Policy Name	Priority	Status	Description	Type	Last Modified	# Ph...	Labels	Watch List
<input checked="" type="checkbox"/>	test_policy	LOCKDOWN - 1	Active		LOCKDOWN	2017-01-26 下午2...	0	TMMS_Security_20170224000_dangero...	0
<input type="checkbox"/>	mobiletest	SECURITY - 1	Active	descripion	SECURITY	2017-02-24 下午2...	0		0
<input type="checkbox"/>	testpolicy	SINGLEAPPMO...	Active		SINGLEAPPM...	2017-03-27 下午1...	0		0
<input type="checkbox"/>	Default AppConn...	APPCONNECT	Active	Default AppConne...	APPCONNECT	2008-01-01 下午4...	8		0

## 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.

The screenshot shows the 'Communication Server Settings' page in the Trend Micro Mobile Security for Enterprise console. The page has a red navigation bar with tabs: Dashboard, Devices, Users, Policies, Applications, Notifications & Reports, Administration, and Help. The 'Administration' tab is selected, and the breadcrumb trail is 'You are here: Administration > Communication Server Settings'. The main content area is titled 'Communication Server Settings' and contains several sections:

- Communication Server:** A dropdown menu for 'Select a Communication Server' is set to 'Local Communication Server'.
- Communication Server Setup Package:** A link 'Click here to download' with an information icon.
- Settings for Communication Between Communication Server and Mobile Devices:** Includes fields for 'External domain name or IP address' (10.64.66.124), 'HTTP port' (8080), and 'HTTPS port' (4343). There is a checkbox for 'Enable HTTPS if there will be iOS or Windows Phone devices in your group'.
- Settings for Communication Between Communication Server and Management Server:** Includes fields for 'Communication Server name or IP address' (10.64.66.124) and 'HTTPS Port' (4343).

At the bottom, there are 'Save' and 'Reset' buttons.

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.

The screenshot shows the 'Deployment Settings' page in the Trend Micro Mobile Security for Enterprise console. The page has a red navigation bar with tabs: Dashboard, Devices, Users, Policies, Applications, Notifications & Reports, and Administration. The 'Administration' tab is selected, and the breadcrumb trail is 'You are here: Administration > Deployment Settings'. The main content area is titled 'Deployment Settings' and contains several sections:

- Server:** A tabbed interface with 'Server', 'Android Agent', and 'iOS Agent' tabs. The 'Server' tab is selected.
- Full Version (Mobile Device Management + Security Scan):** A radio button option. Description: 'Provides security scan for Andoird, iOS and Windows Phone mobile devices, and includes mobile device management (MDM) features.'
- Security Scan:** A radio button option. Description: 'Provides security scan for Android and iOS mobile devices while enabling integration with other mobile device management (MDM) solu'.
- MDM Solution:** A dropdown menu showing 'MobileIron Core On-Premise'.
- Service:** A dropdown menu showing 'Unlisted', 'AirWatch', 'MobileIron Core Hosted', and 'MobileIron Core On-Premise'.
- Configure:** A dropdown menu showing 'MobileIron Core On-Premise'.

At the bottom, there is a link 's to access MobileIron server'.

5. Under Register Service, configure the following AirWatch settings:

- API URL
- API KEY
- Account Name
- Password

#### Deployment Settings

---

Server

Android Agent

iOS Agent

☐ Full Version (Mobile Device Management + Security Scan)  
Provides security scan for Andoird, iOS and Windows Phone mobile devices, and includes mobile device management (MDM) features.

☒ Security Scan  
Provides security scan for Android and iOS mobile devices while enabling integration with other mobile device management (MDM) solutions

MDM Solution 

MobileIron Core On-Premise ▾

Service Registration

Configure following authentication settings to access MobileIron server

API URL 

https://m.mobileiron.net/trendmicro4813 ⓘ

Account Name 

admin

Password 

.....

Verify Settings

Last verified:

Data Synchronization Settings

Security Category Prefix 

Prefix\_TMMS ⓘ

☐ Enable Data Synchronization

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

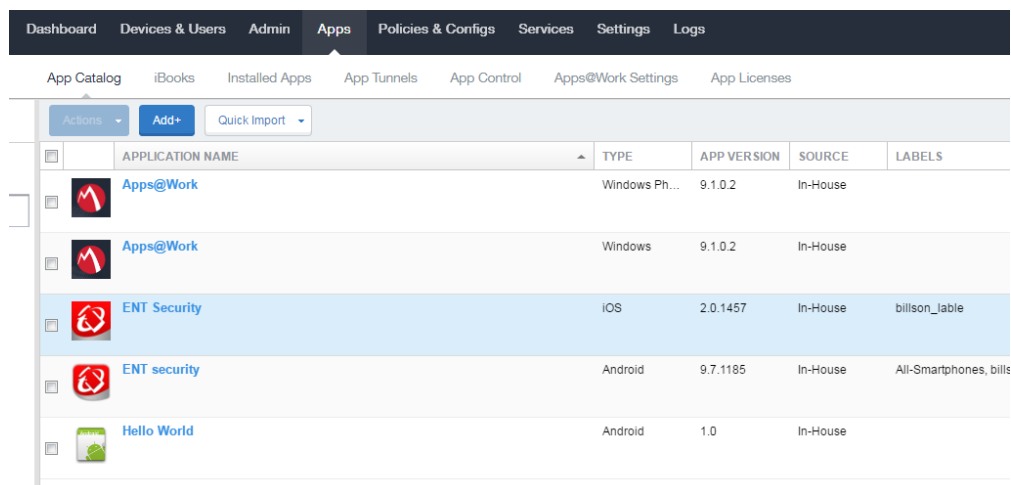
## 1.4.2 Deploy Android agent

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

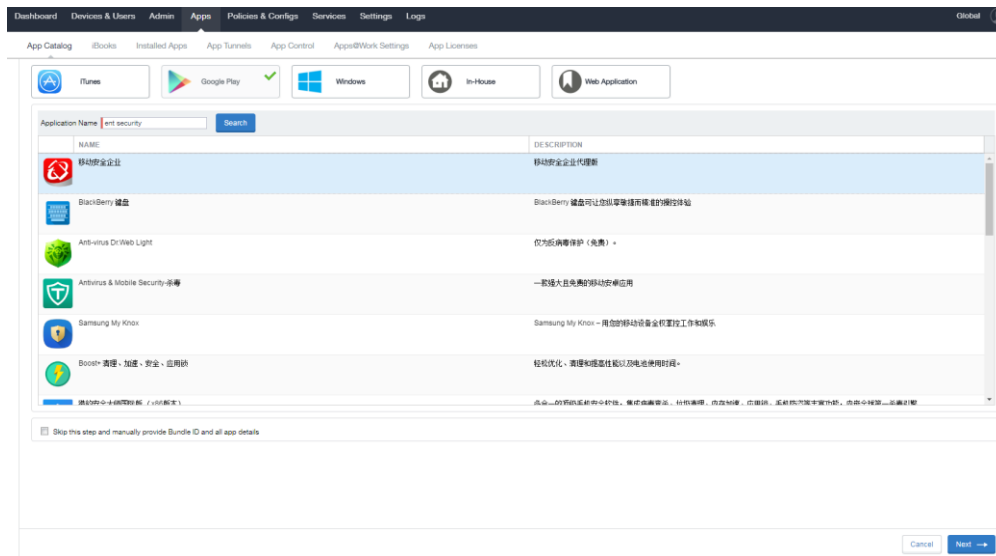
Version	Pros and Cons
Google play version	Administrator will need to send an email to the end-user with QR code or Enrollment Key. End-users need to open TMMS agent and scan the QR code or manually enter the Enrollment Key to register their device to server. Agent can be updated automatically.
TMMS server version	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.

## Google Play build

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



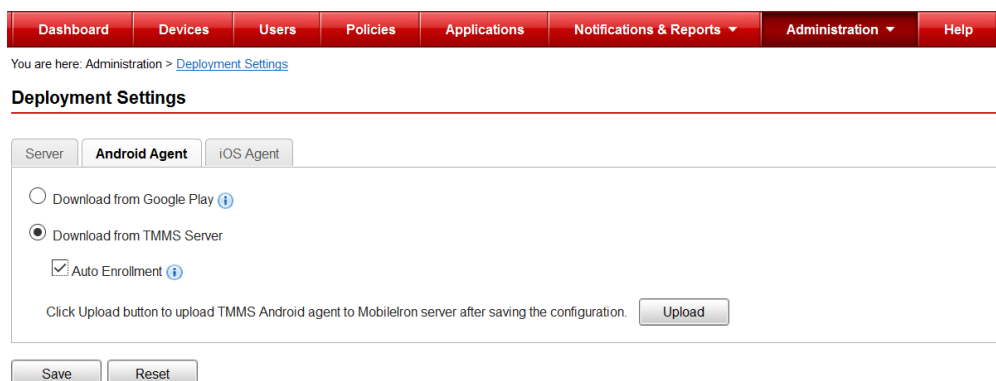
2. Click **Google Play**, search for "ent security", then select **Mobile Security for Enterprise**.



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**.



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**.

Dashboard

Devices

Users

Policies

Applications

Notifications & Reports

Administration

Help

You are here: Administration > [Device Enrollment Settings](#)

### Device Enrollment Settings

Authentication

Agent Installation

Terms of Use Customization

#### User Authentication

☐

Authenticate using Active Directory

(Click [here](#) to configure Active Directory)

☒

Authenticate using Enrollment Key

Generate and send an enrollment key to invited users

Enrollment Key usage limitation 

Use for multiple times

☐ Enrollment Key expires after 

7 days

☒ Use preset Enrollment Key


Enrollment Key 

C695I52WAW

Generate

☐ Enrollment Key expires on 

18/01/2017



Scan the QR code to enroll device using the preset enrollment key.

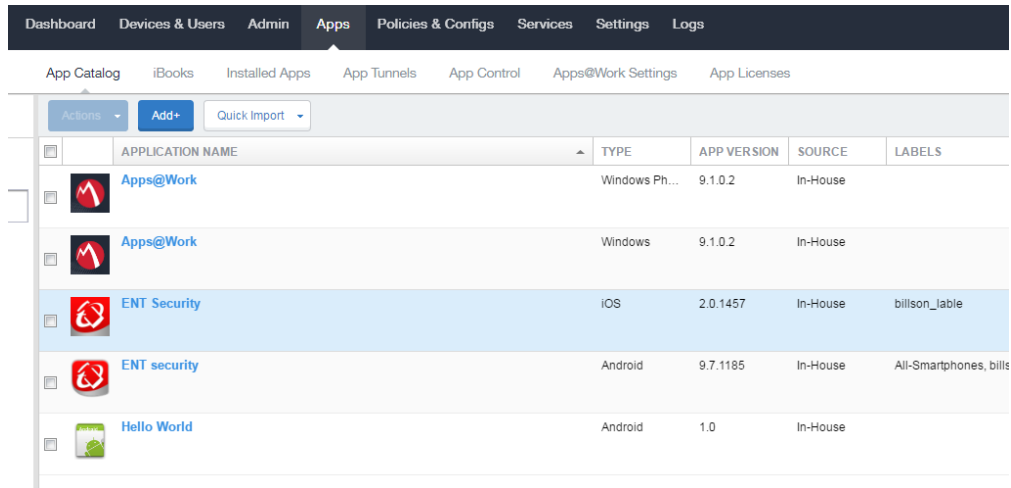
Save

Reset

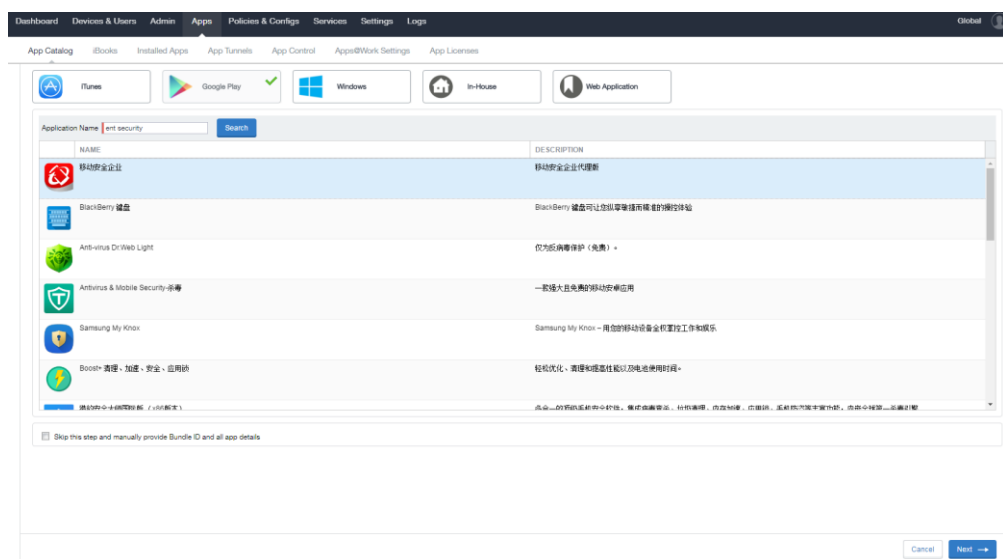


## 1.4.3 Deploy IOS agent

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

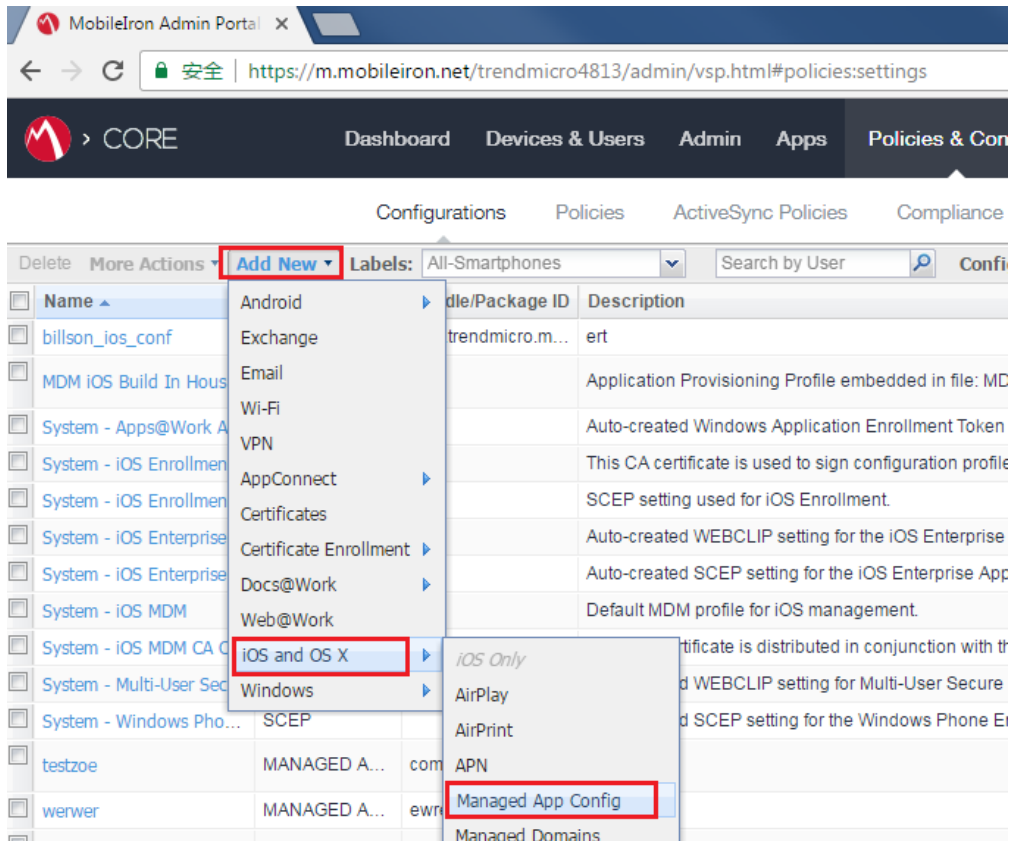


2. Click **iTunes**, search for "ent security", then select **Mobile Security for Enterprise**.



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.

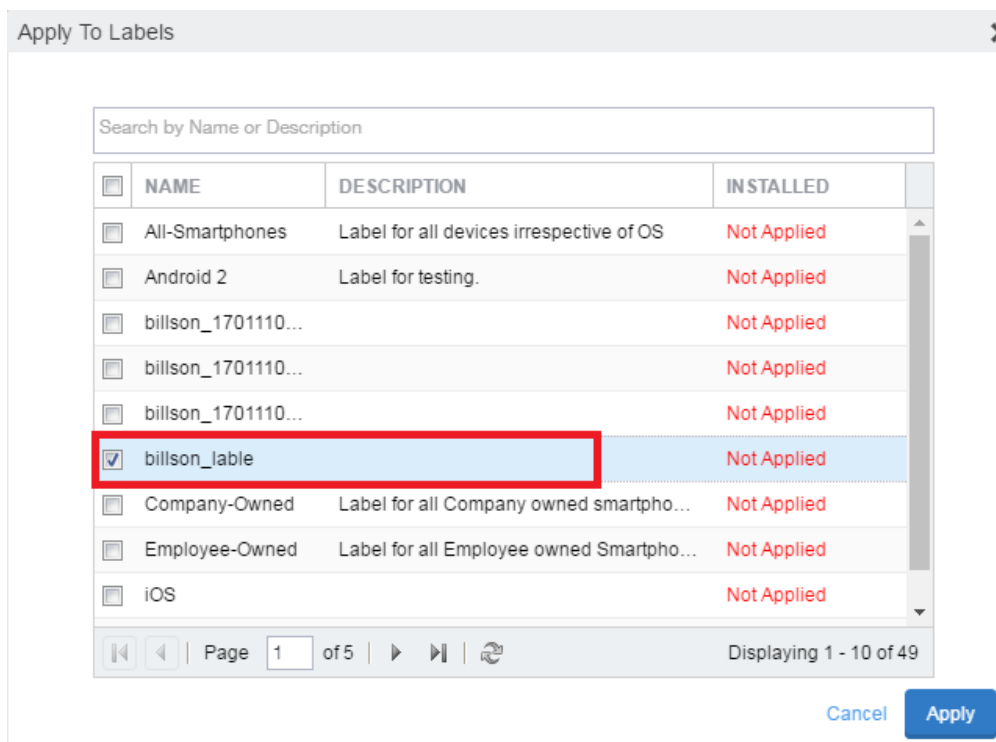


14. Enter the name, description, TMMS agent bundle ID, and select the configuration file downloaded from Step 2: Configure TMMS for the integration.

The screenshot shows the 'New Managed App Config Setting' form. The form fields are: Name (test\_ios\_config), Description (this is a test ios app config), BundleId (com.trendmicro.mdmhouse.entse), and File (mobileiron\_ios.plist). The 'Save' button is highlighted in blue.

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.

