Contents

1 Introduction

There are two major function categories in TMMS: One is mobile device management (MDM) related features and the other is security related features.

The MDM application needs to be installed with an MDM profile on an Apple device. As a MDM solution, TMMS also need to install a profile on an Apple device.

Apple devices only allow one MDM profile to be installed. If there are other MDM solutions that need to be installed, we can provide TMMS "Security Only" Mode.

- TMMS security scan mode only have security scan related functions, that's why it will not install MDM profile. The latest 9.7 version can integrate with AirWatch and MobileIron, the latest 9.8 sp1 can integrate with CITRIX XENMOBILE and IBM MAAS360
- CITRIX XENMOBILE is a Mobile Device Management (MDM) software for manage devices, content, applications and email.

To provide security information in the 3rd party MDM console, TMMS security only mode will share security information to the 3rd party MDM, then the mobile administrator can see the security information from the 3rd party MDM console.

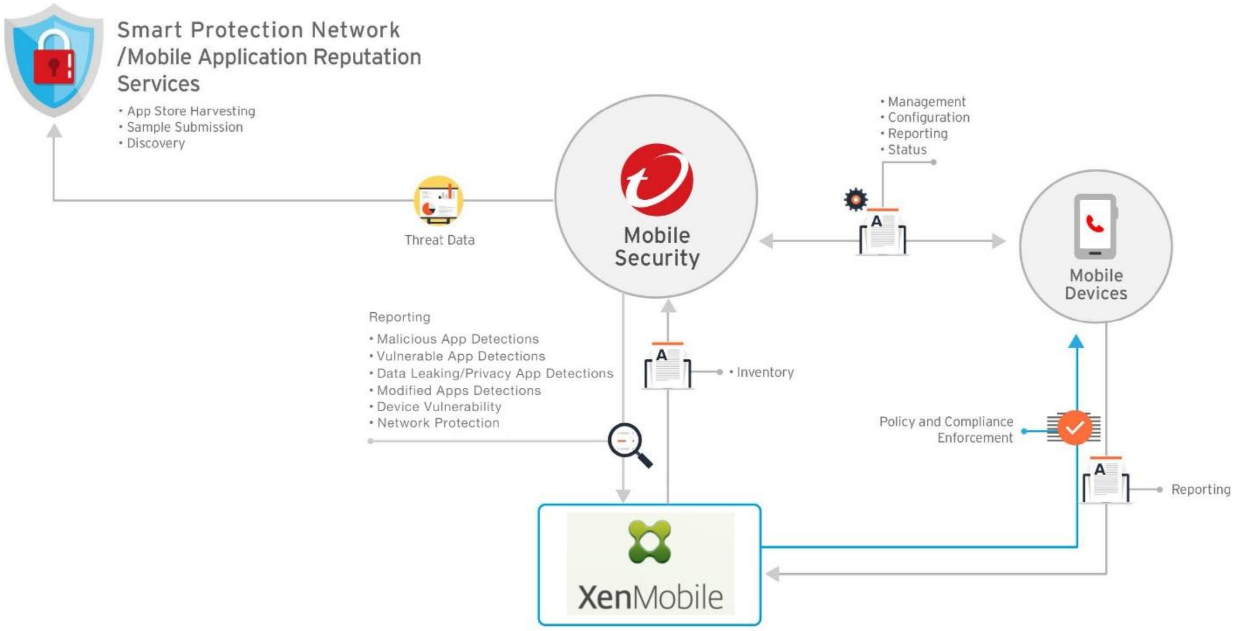
This document gives detailed steps for how to integration with CITRIX XENMOBILE.

1.1 Requirements

The following requirements/conditions should be met before proceeding:

- Mobile Security for Enterprise 9.8 sp1 version or later
- The communication server is configured to either Local Communication server or Cloud Communication Server.
- CITRIX XENMOBILE 10.6.0.22 and later

1.2 Architecture



- **Mobile App Reputation Services(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

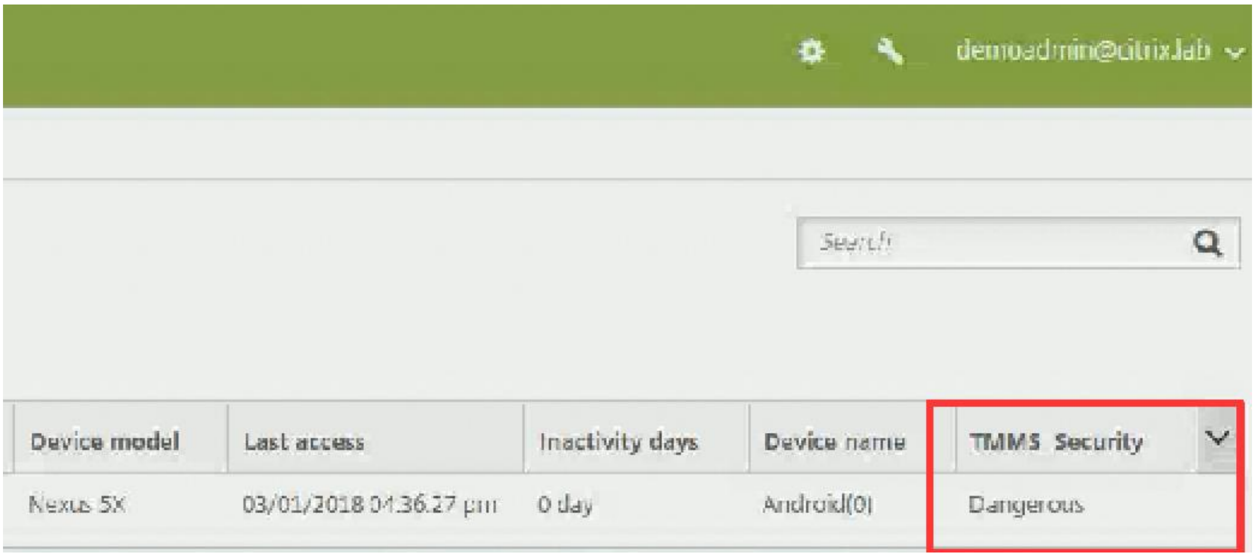
- **Smart Protection Network(SPN)**

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 Device Compliance status

The Citrix XenMobile Console provides a list of enrolled devices, showing the device's compliance status.



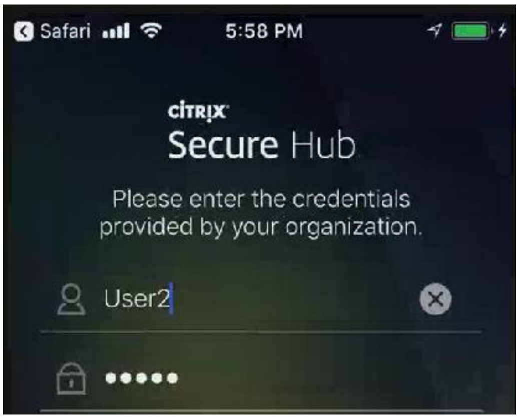
Device model	Last access	Inactivity days	Device name	TMMS Security
Nexus 5X	03/01/2018 04:36:27 pm	0 day	Android(0)	Dangerous

1.4 Basic Deployment

1.4.1 Prepare Citrix XenMobile account

We need to have an Citrix XenMobile account to be used for the communication between the TMMS server and Citrix XenMobile. The user will need the administrator permissions on Citrix XenMobile.

Add device in XenMobile and then enroll the device to XenMobile first, TMMS will use XenMobile agent to install mobile security agent for Android and IOS.



Please enter the credentials provided by your organization.

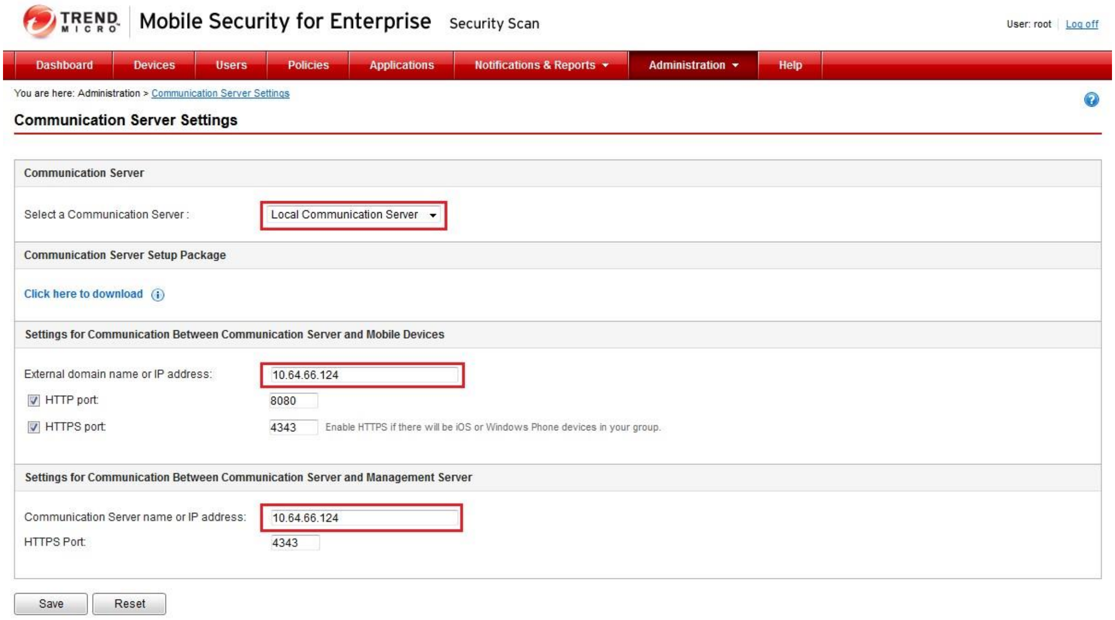
User2

•••••

1.4.2 TMMS Server Settings

1. Log on to the Mobile Security Administration web console.
2. Click **Administration** > **Communication Server Settings** on the menu bar, 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.

   Note: (only Local Communication Server support this integration, Cloud Communication Server does not support integration with XenMobile)



You are here: Administration > Communication Server Settings

Communication Server Settings

Communication Server

Select a Communication Server : Local Communication Server

Communication Server Setup Package

Click here to download

Settings for Communication Between Communication Server and Mobile Devices

External domain name or IP address: 10.64.66.124

☑ HTTP port: 8080

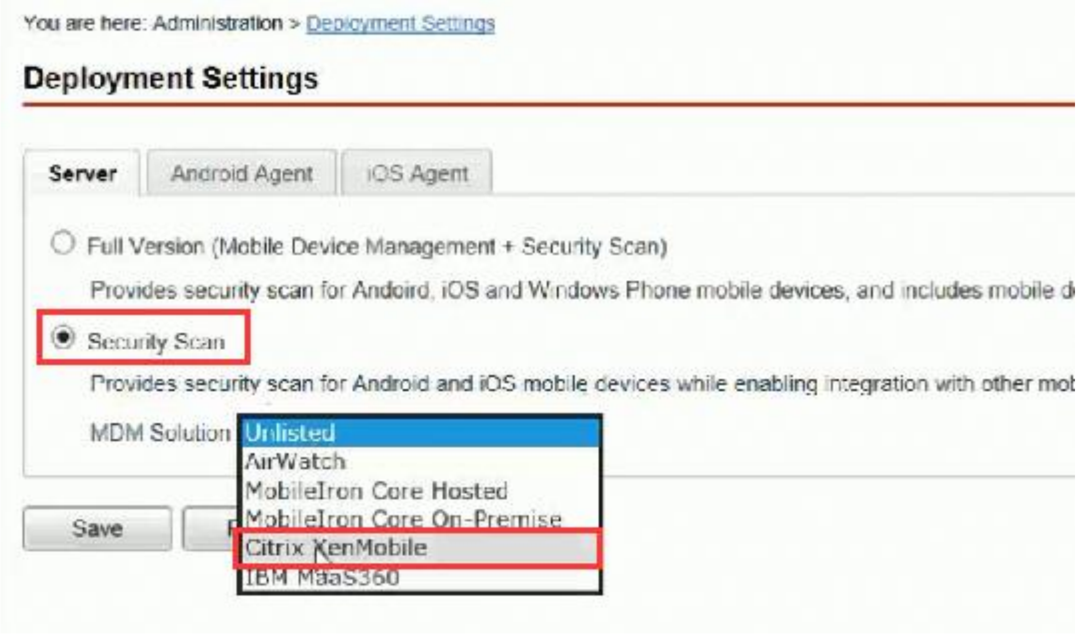
☑ HTTPS port: 4343 Enable HTTPS if there will be iOS or Windows Phone devices in your group.

Settings for Communication Between Communication Server and Management Server

Communication Server name or IP address: 10.64.66.124

HTTPS Port: 4343

3. Click **Administration** > **Deployment Settings**.
4. Under the Server tab, select **Security Scan**, and then select **Citrix XenMobile** as the MDM Solution from the drop down list.



You are here: Administration > Deployment Settings

Deployment Settings

○ Full Version (Mobile Device Management + Security Scan)

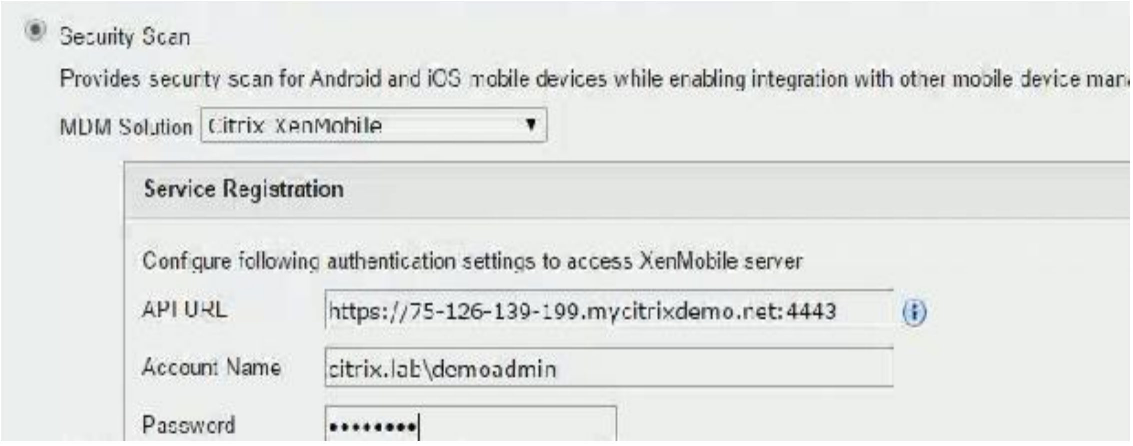
Provides security scan for Andoird, iOS and Windows Phone mobile devices, and includes mobile d

● Security Scan

Provides security scan for Android and iOS mobile devices while enabling integration with other mot

MDM Solution: Unlisted

5. Under Register Service, configure the following Citrix XenMobile settings:
    - API URL
    - account Name, the account used in the integration feature should have "Citrix XenMobile administrator" role privilege.
    - Password



● Security Scan

Provides security scan for Android and iOS mobile devices while enabling integration with other mobile device man

MDM Solution: Citrix XenMobile ▼

Service Registration

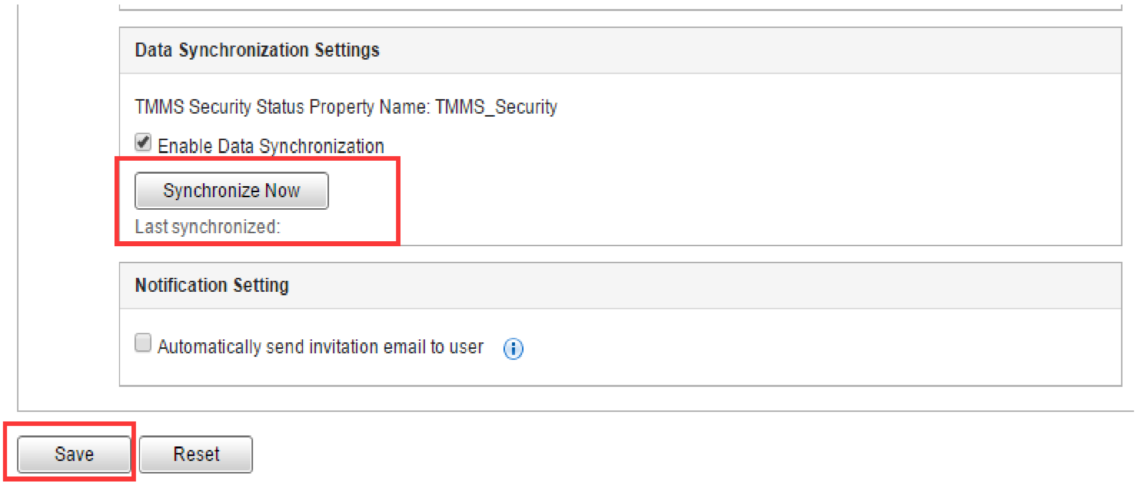
Configure following authentication settings to access XenMobile server

API URL: https://75-126-139-199.mycitrixdemo.net:4443

Account Name: citrix.lab\demoadmin

Password: ••••••••

6. Click **Verify Settings** to make sure Mobile Security can connect to the Citrix XenMobile server.
7. After connection has been verified, please click Synchronize and Save to update data from XenMobile and save settings in TMMS



Data Synchronization Settings

TMMS Security Status Property Name: TMMS_Security

☑ Enable Data Synchronization

Last synchronized:

Notification Setting

☐ Automatically send invitation email to user

1.4.3 Deploy Android agent

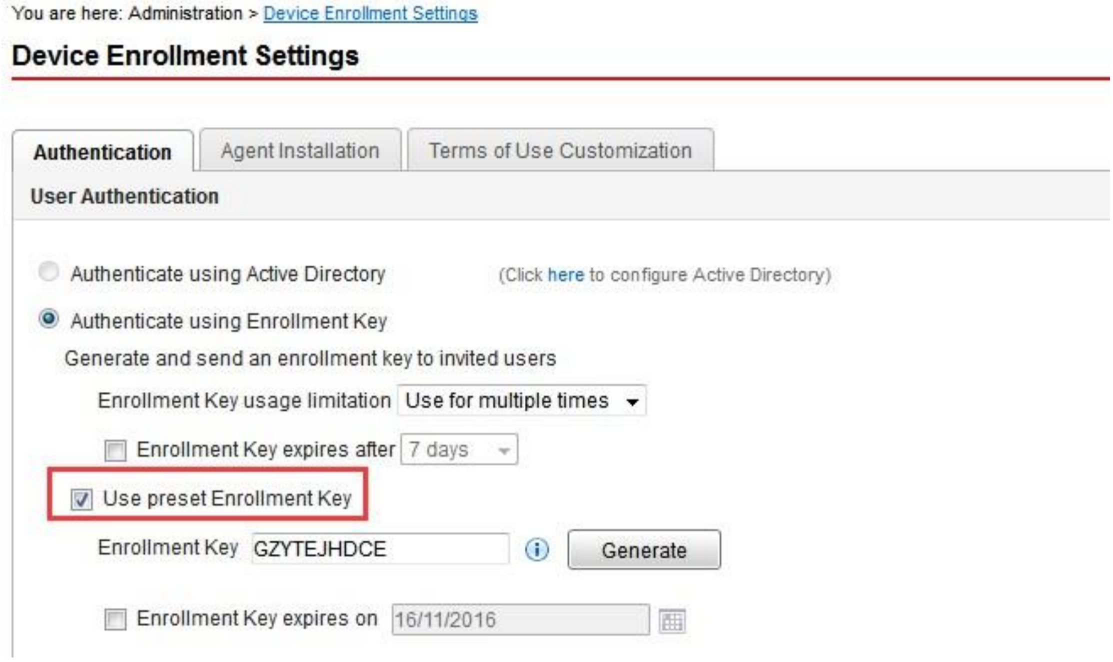
TMMS has two Android agent versions. Citrix XenMobile Administrator need to choose one of the following versions:

Version	Pros and Cons

Google play version	Administrator need to send an email to 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. Tick **Use preset Enrollment Key**, so the application can be enrolled with this key



You are here: Administration > Device Enrollment Settings

Device Enrollment Settings

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

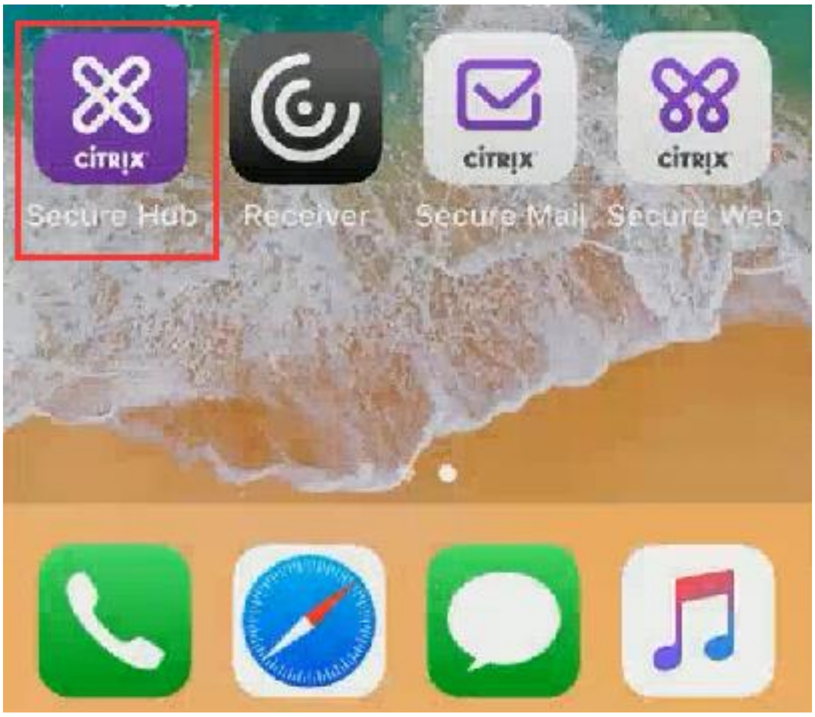
□ Enrollment Key expires after 7 days

☑ Use preset Enrollment Key

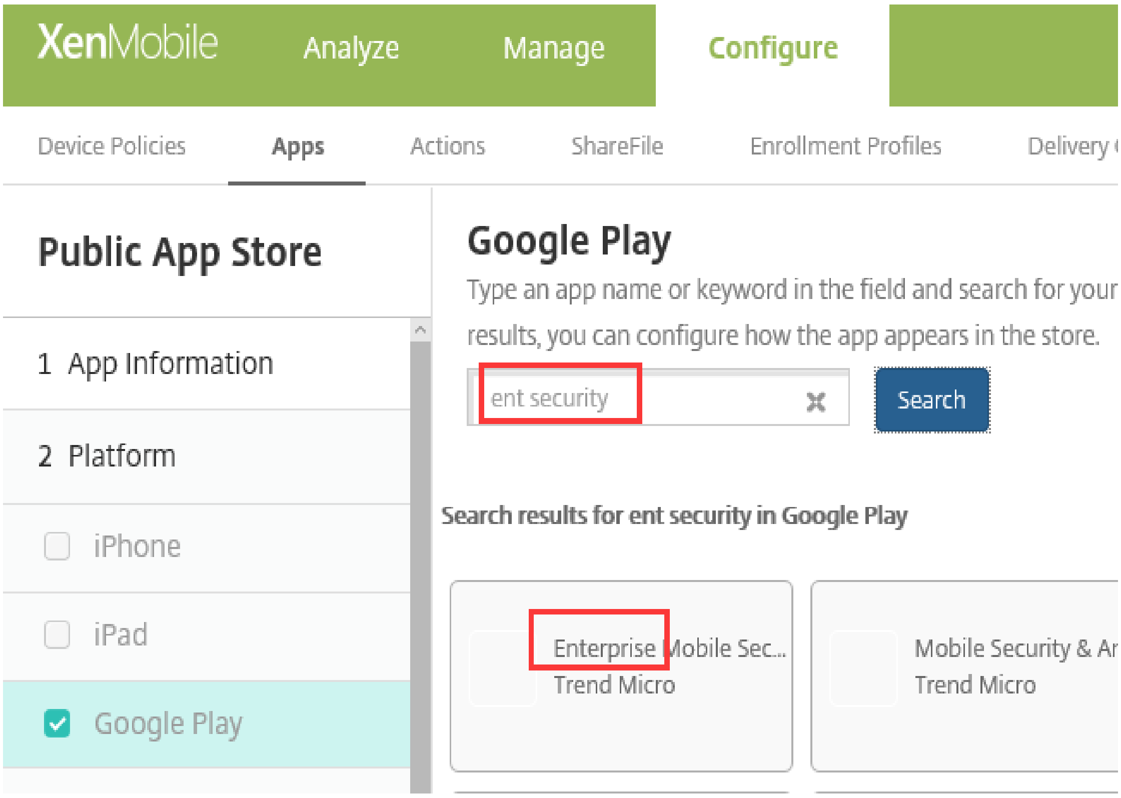
Enrollment Key: GZYTEJHDCE

□ Enrollment Key expires on 16/11/2016

2. Deploy XenMobile agent and then launch it. Log on to Citrix XenMobile agent console



3. On the XenMobile web console, add Trendmicro Mobile Security from Google play store, please set the deploy scope and schedule.



Public App Store

1 App Information

2 Platform

□ iPhone

□ iPad

☑ Google Play

Google Play

Type an app name or keyword in the field and search for your results, you can configure how the app appears in the store.

ent security

Search

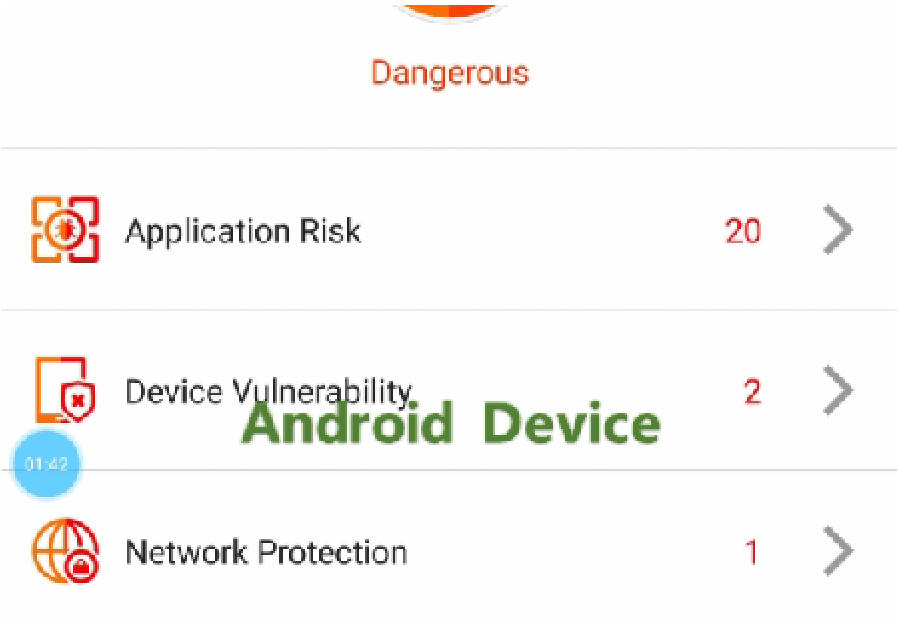
Search results for ent security in Google Play

Enterprise Mobile Sec... Trend Micro

Mobile Security & Ar Trend Micro

4. On the XenMobile agent console, please install Enterprise Mobile Security agent application:

5. After download and install the Mobile security application, please launch the mobile security application, then scan QR code to enroll device to TMMS server, while doing security scan and found security issue, the information will report to TMMS server and redirect to Citrix XenMobile.



Dangerous

Application Risk 20

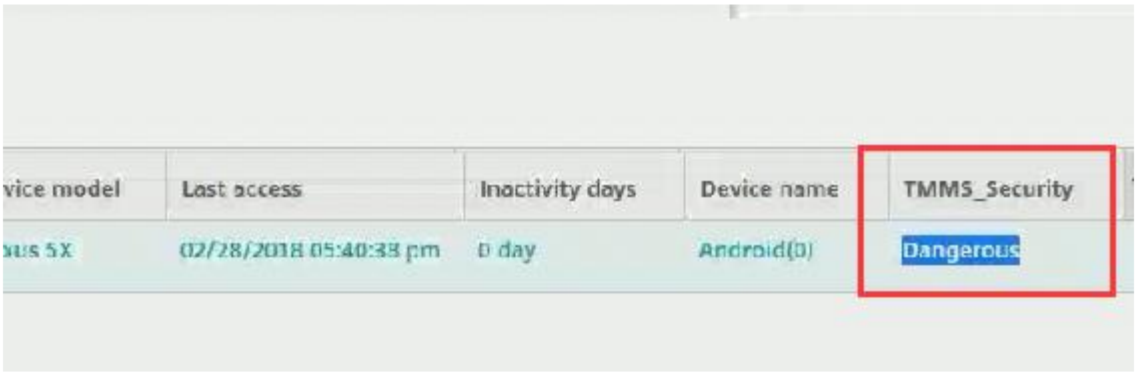
Device Vulnerability 2

Android Device

01:42

Network Protection 1

TMMS agent console

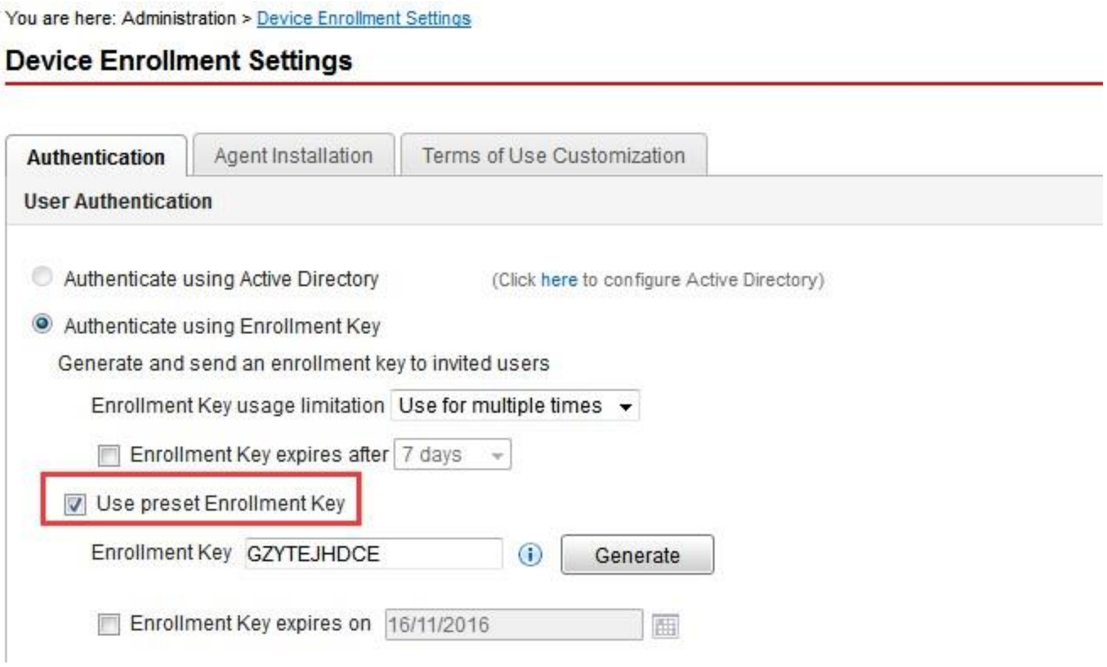


vice model	Last access	Inactivity days	Device name	TMMS_Security
ous 5X	02/28/2018 05:40:33 pm	0 day	Android(0)	Dangerous

Found in XenMobile console

Local Server build

1. Tick **Use preset Enrollment Key**.



You are here: Administration > Device Enrollment Settings

Device Enrollment Settings

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

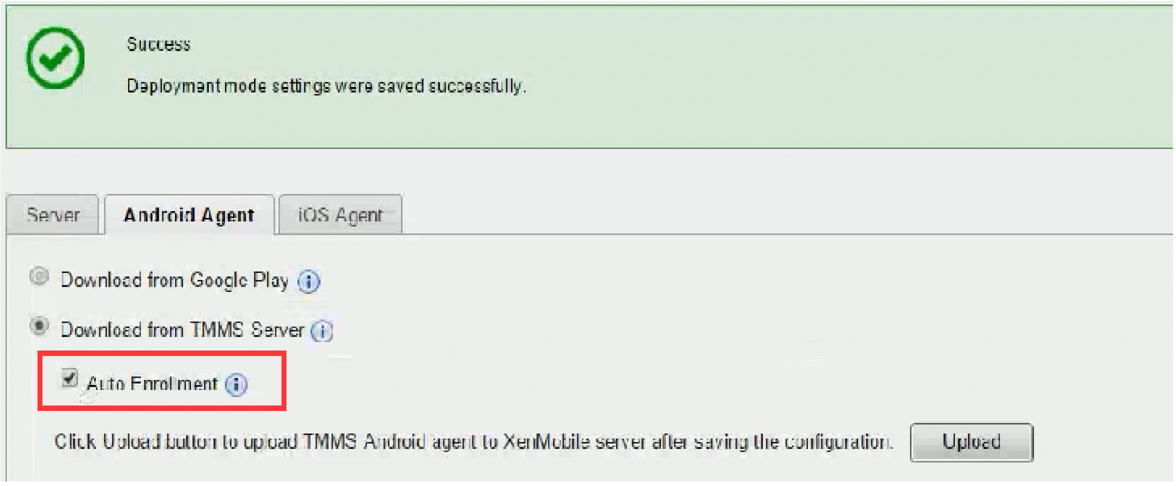
☑ Use preset Enrollment Key

Enrollment Key: GZYTEJHDCE

□ Enrollment Key expires on 16/11/2016

2. In the TMMS for Enterprise web console, go to **Administration** > **Deployment Settings** > **Android Agent**.
3. Choose **Download from TMMS Server**.

   Tick **Auto Enrollment**.



Success

Deployment mode settings were saved successfully.

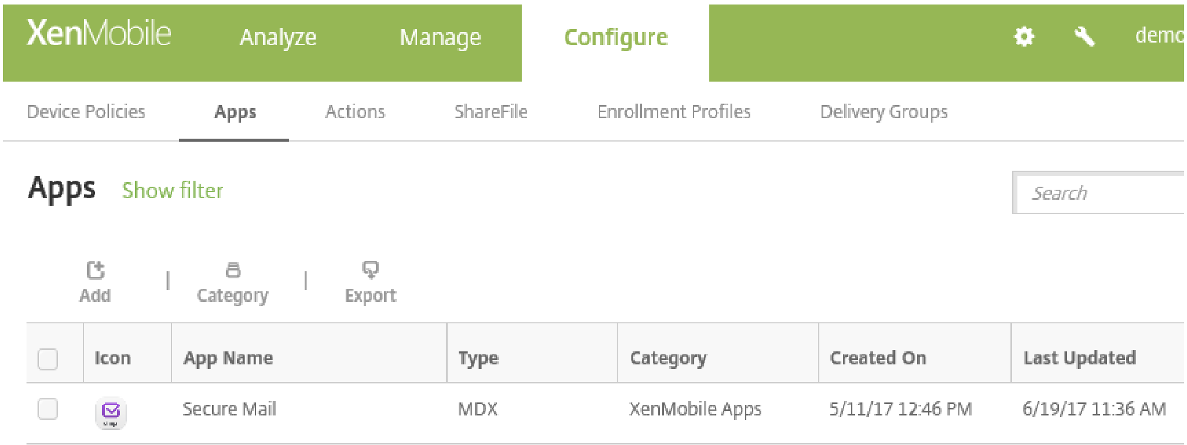
○ Download from Google Play

● Download from TMMS Server

☑ Auto Enrollment

Click Upload button to upload TMMS Android agent to XenMobile server after saving the configuration.

4. Click upload, this action will upload TMMS application to Citrix XenMobile server. The application can be found at this place.



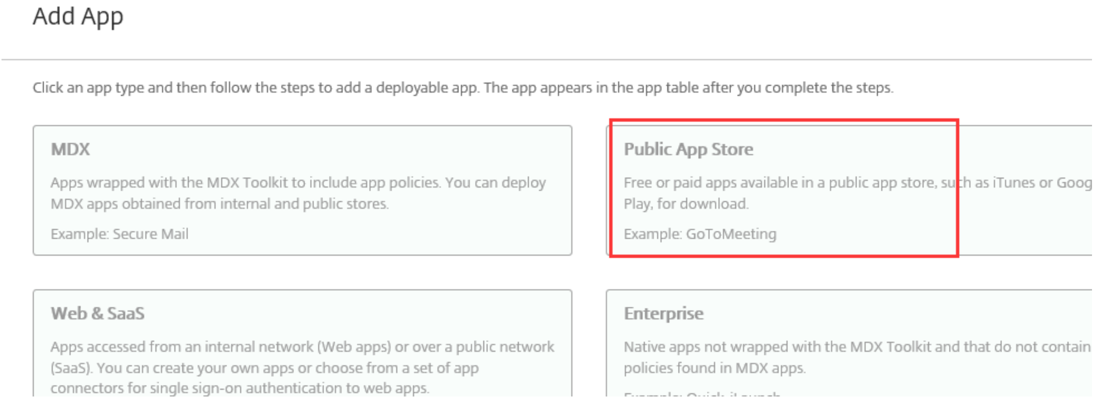
□	Icon	App Name	Type	Category	Created On	Last Updated
□		Secure Mail	MDX	XenMobile Apps	5/11/17 12:46 PM	6/19/17 11:36 AM

5. Find the application and schedule the deploy for TMMS mobile security.
6. After the application has been deployed, TMMS mobile security will do schedule scan for the devices and report device status to the Citrix server. Let end-user launch the mobile security application, then the device will be enrolling to server. it also has real-time scan, while install new application, TMMS will scan and report to server too.

1.4.4 Deploy IOS agent

1. Login to the Citrix XenMobile Admin console, add Trendmicro mobile security from Apple store

   Under the **Add** Application page, please choose public app store



Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: Secure Mail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Goog Play, for download.

Example: GoToMeeting

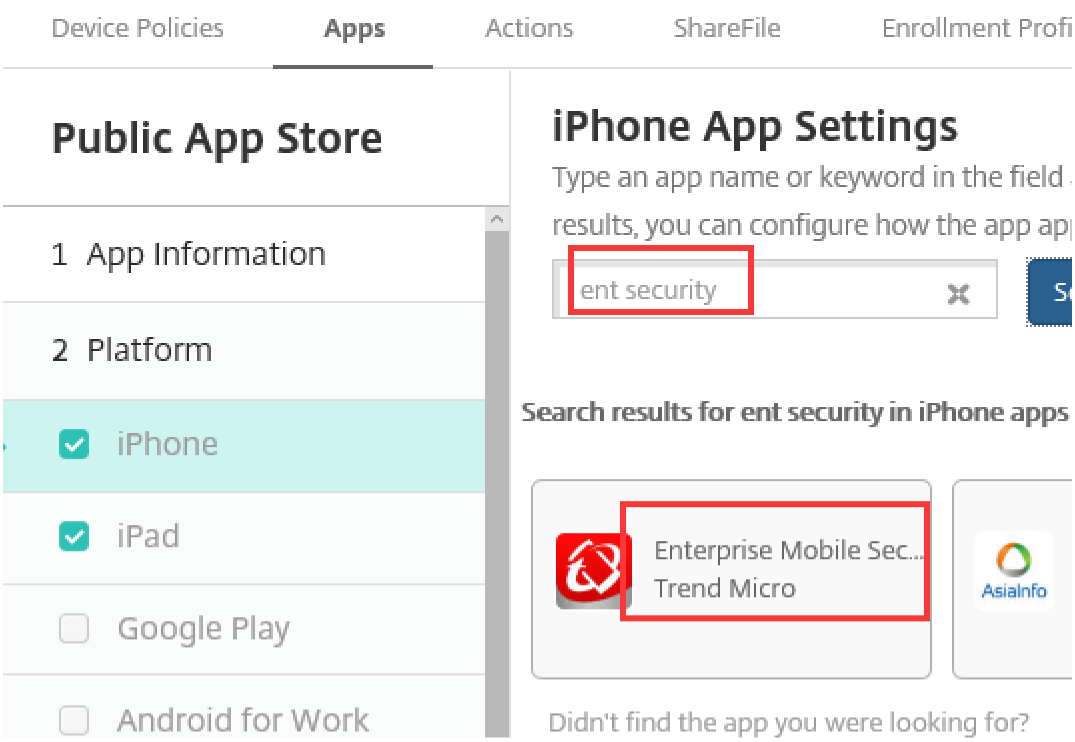
Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain policies found in MDX apps.

2. Choose iPhone and iPad, and then search **Ent Security**



Public App Store

1 App Information

2 Platform

☑ iPhone

☑ iPad

□ Google Play

□ Android for Work

iPhone App Settings

Type an app name or keyword in the field
results, you can configure how the app ap

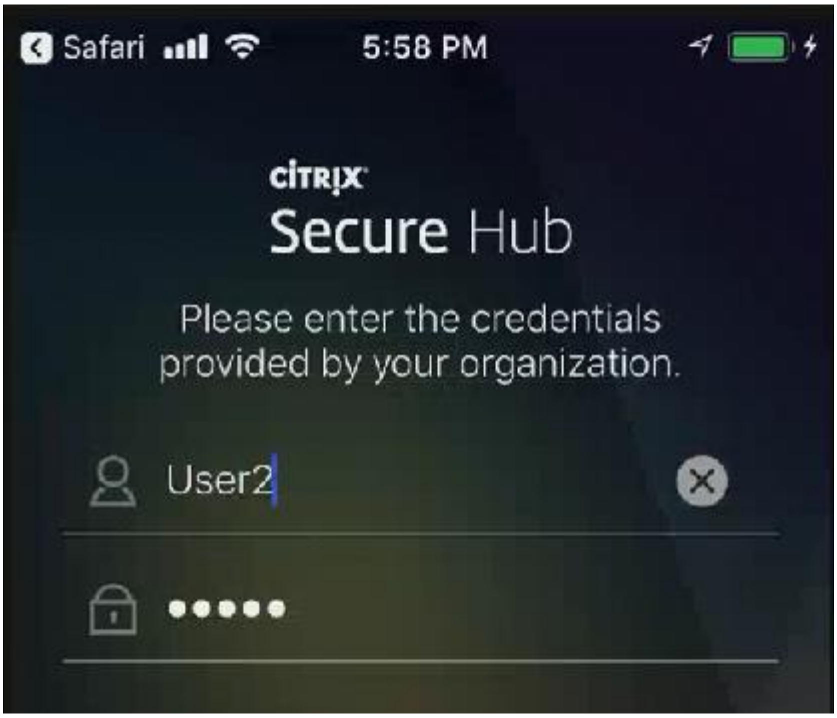
ent security

Search results for ent security in iPhone apps

Enterprise Mobile Sec...
Trend Micro

Didn't find the app you were looking for?

3. Follow the wizard to set the deployment and schedule plan.
4. On the Apple device, install Citrix XenMobile agent and enroll the device to Citrix XenMobile server

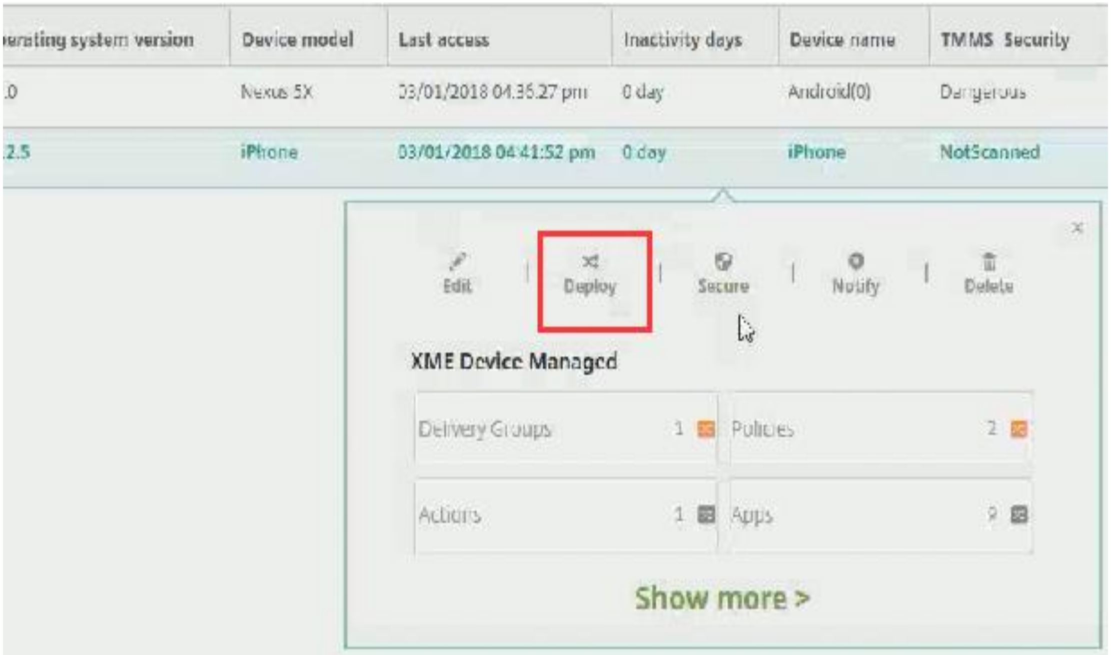


Please enter the credentials provided by your organization.

User2

•••••

5. Configure from the web console to deploy the mobile security application, wait Citrix XenMobile application to install the mobile security agent

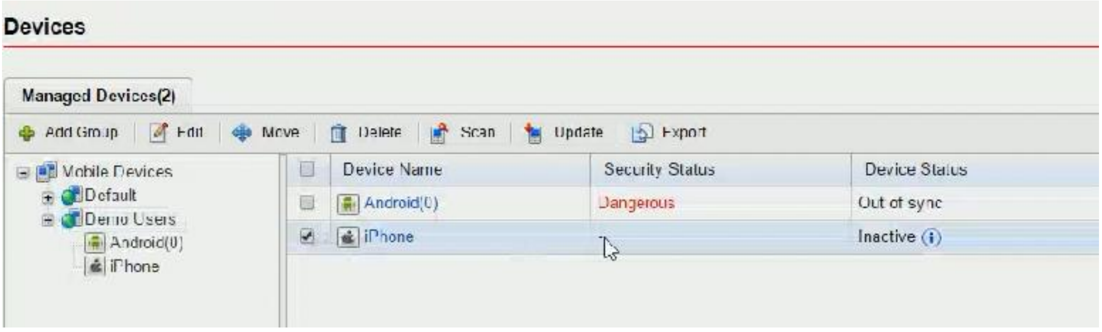


erating system version	Device model	Last access	Inactivity days	Device name	TMMS Security
.0	Nexus 5X	03/01/2018 04:35:27 pm	0 day	Android(0)	Dangerous
2.5	iPhone	03/01/2018 04:41:52 pm	0 day	iPhone	NotScanned

XME Device Managed

Delivery Groups 1	Policies 2
Actions 1	Apps 9

6. After the application is installed on the Apple device, you can go to Deployment Settings page click data sync button, then you can find this device from TMMS management console



Devices

Managed Devices(2)

□	Device Name	Security Status	Device Status
□	Android(0)	Dangerous	Out of sync
☑	iPhone		Inactive (i)

7. Do a scan on device, if there are malware found, it will be set to dangerous on Citrix XenMobile console

TMMS will also do schedule scan, the Citrix XenMobile administrator can check the scan result from web console too.