TREND MICRO™

9.8 TREND MICRO™ Mobile Security™

Service Pack 5 Critical Patch 3

Administrator's Guide

(for Security Scan Deployment Mode)

Comprehensive security for enterprise handhelds

Endpoint Security

Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com

Trend Micro, the Trend Micro t-ball logo, OfficeScan, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2022. Trend Micro Incorporated. All rights reserved.

Document Part No.: TSEM99590/220830

Release Date: September 2022

Protected by U.S. Patent No.: Patents pending.

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Evaluate this documentation on the following site:

https://www.trendmicro.com/download/documentation/rating.asp

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Trend Micro Mobile Security for Enterprise collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Notice:

https://www.trendmicro.com/privacy

Table of Contents

Preface

Preface vii

Audience viii

Mobile Security Documentation viii

Document Conventions ix

Chapter 1: Introduction

Understanding Mobile Threats 1-2

About Trend Micro Mobile Security 1-2

About Machine Learning in Trend Micro Mobile Security 1-2

Architecture of Mobile Security System 1-3

Components of Mobile Security System 1-3

Comparison Between Local and Cloud Communication Servers 1-6

What's New in Release 9.8 SP5 Critical Patch 3 1-6

What's New in Release 9.8 SP5 Critical Patch 2 1-7

What's New in Release 9.8 SP5 Critical Patch 1 1-7

What's New in Release 9.8 SP5 1-7

What's New in Release 9.8 SP4 1-8

What's New in Release 9.8 SP3 1-8

What's New in Release 9.8 SP2 Patch 1 1-9

What's New in Release 9.8 SP2 1-9

What's New in Release 9.8 SP1 1-10

What's New in Release 9.8 1-10

What's New in Release 9.7 Patch 3 1-11

What's New in Release 9.7 Patch 2 1-11
What's New in Release 9.7 1-12
What's New in Release 9.6 SP1 1-13
What's New in Release 9.6 1-14
Main Mobile Device Agent Features 1-15
Supported Mobile Device OS Features 1-16

Chapter 2: Getting Started with Mobile Security

Administration Web Console 2-2
Accessing the Administration Web Console 2-2
Turning Off Compatibility Mode in Internet Explorer 2-4
Product License 2-4
Dashboard Information 2-5
Customizing the Dashboard 2-6
Administration Settings 2-9
Configuring Active Directory (AD) Settings 2-9
Configuring User Authentication 2-9
Configuring Database Settings 2-9
Configuring Communication Server Settings 2-10
Configuring Deployment Settings 2-10
Managing Administrator Accounts 2-11
Command Queue Management 2-18
Configuring Schedule for Deleting Old Commands 2-19
Deleting Old Commands Manually 2-20
Managing Certificates 2-20
Uploading a Certificate 2-20
Deleting a Certificate 2-21

Chapter 3: Integrating with Other MDM Solutions

Feature Integration Comparison for MDM Solutions 3-2
Integration with AirWatch 3-3
Prerequisites for Integration 3-3

AirWatch Integration Architecture 3-3
Integration Features 3-4
AirWatch Account Permission Requirements for Integration 3-7
Configuring AirWatch Integration 3-9
Agent Deployment 3-11

Integration with MobileIron 3-17
Prerequisites for Integration 3-17
MobileIron Integration Architecture 3-17
Integration Features 3-18
Configuring MobileIron Integration 3-20
Agent Deployment 3-21

Integration with Citrix XenMobile 3-25
Prerequisites for Integration 3-25
Citrix XenMobile Integration Architecture 3-25
Integration Features 3-26
Configuring Citrix XenMobile Integration 3-28
Agent Deployment 3-29

Integration with IBM MaaS360 3-34
Prerequisites for Integration 3-34
IBM MaaS360 Integration Architecture 3-34
Integration Features 3-35
Configuring IBM MaaS360 Integration 3-36
Agent Deployment 3-37

Integration with BlackBerry UEM 3-41
Prerequisites for Integration 3-42
BlackBerry UEM Integration Architecture 3-42
Integration Features 3-43
Configuring BlackBerry UEM Integration 3-43
Agent Deployment 3-44

Chapter 4: Managing Mobile Devices

Managed Devices Tab 4-2
Groups in Mobile Security 4-2
Managing Groups 4-2

Managing Mobile Devices 4-4
Mobile Device Status 4-7

Mobile Device Agent Tasks 4-9
Updating Mobile Device Agents 4-10
Updating Mobile Device Information 4-10
Exporting Data 4-11

Integration with Trend Micro Control Manager 4-12
Creating Security Policies in Control Manager 4-12
Deleting or Modifying Security Policies 4-12
Security Policy Statuses on Control Manager 4-13

Chapter 5: Viewing Users

Users Tab 5-2
Viewing the Users List 5-2

Chapter 6: Protecting Devices with Policies

About Policies 6-2

Policies for All Devices 6-2
Application Approved List 6-2
Trusted Network Traffic Decryption Certificate List 6-3
Managing Policies for All Devices 6-3

Policies for All Groups 6-6
Common Policy 6-6
Security Policy 6-7
Managing Policies for All Groups 6-10

Chapter 7: Viewing and Managing Detections

About Suspicious Applications Screen 7-2
Viewing Suspicious Android Applications 7-4
Viewing Suspicious iOS Applications 7-5

Viewing Malicious SSL Certificates 7-6

Viewing Malicious iOS Profiles 7-7

Chapter 8: Updating Components

About Component Updates 8-2
Updating Mobile Security Components 8-2
Manual Update 8-2
Scheduled Update 8-3
Specifying a Download Source 8-4
Manually Updating a local AU server 8-5

Chapter 9: Viewing and Maintaining Logs

About Logs 9-2
Viewing Mobile Device Agent Logs 9-2
Log Maintenance 9-4
Scheduling Log Deleting 9-5
Deleting Logs Manually 9-5

Chapter 10: Using Notifications and Reports

About Notification Messages and Reports 10-2
Configuring Notification Settings 10-2
Configuring Email Notifications 10-2
Administrator Notifications 10-3
Enabling Administrator Notifications 10-3
Configuring Administrator Notification Settings 10-4
Reports 10-4
Generating Reports 10-5
Viewing Reports 10-6
Sending Reports 10-7
Scheduling Reports 10-8
Modifying the Email Template 10-8
User Notifications 10-9
Configuring User Notifications 10-9

Chapter 11: Technical Support

Troubleshooting Resources 11-2
Using the Support Portal 11-2
Threat Encyclopedia 11-2

Contacting Trend Micro 11-3
Speeding Up the Support Call 11-4

Sending Suspicious Content to Trend Micro 11-4
Email Reputation Services 11-4
File Reputation Services 11-5
Web Reputation Services 11-5

Other Resources 11-5
Download Center 11-5
Documentation Feedback 11-6

Index

Index IN-1

Preface

Preface

Welcome to the Trend Micro™ Mobile Security for Enterprise version 9.8 SP5 Critical Patch 3 Administrator's Guide. This guide provides detailed information about all Mobile Security configuration options. Topics include how to update your software to keep protection current against the latest security risks, how to configure and use policies to support your security objectives, configuring scanning, synchronizing policies on mobile devices, and using logs and reports.

This preface discusses the following topics:

- *Audience on page viii*
- *Mobile Security Documentation on page viii*
- *Document Conventions on page ix*

Audience

The Mobile Security documentation is intended for both administrators—who are responsible for administering and managing Mobile Device Agents in enterprise environments—and mobile device users.

Administrators should have an intermediate to advanced knowledge of Windows system administration and mobile device policies, including:

- Installing and configuring Windows servers
- Installing software on Windows servers
- Configuring and managing mobile devices
- Network concepts (such as IP address, netmask, topology, and LAN settings)
- Various network topologies
- Network devices and their administration
- Network configurations (such as the use of VLAN, HTTP, and HTTPS)

Mobile Security Documentation

The Mobile Security documentation consists of the following:

- *Installation and Deployment Guide*—this guide helps you get "up and running" by introducing Mobile Security, and assisting with network planning and installation.
- *Administrator's Guide*—this guide provides detailed Mobile Security configuration policies and technologies.
- *Online help*—the purpose of online help is to provide "how to's" for the main product tasks, usage advice, and field-specific information such as valid parameter ranges and optimal values.
- *Readme*—the Readme contains late-breaking product information that is not found in the online or printed documentation. Topics include a

description of new features, installation tips, known issues, and release history.

- *Knowledge Base*— the Knowledge Base is an online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, open:

  http://esupport.trendmicro.com/

Tip

Trend Micro recommends checking the corresponding link from the Download Center (http://www.trendmicro.com/download) for updates to the product documentation.

Document Conventions

The documentation uses the following conventions.

TABLE 1. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface

Convention	Description
Note	Configuration notes
Tip	Recommendations or suggestions
Important	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options

Chapter 1

Introduction

Trend Micro™ Mobile Security for Enterprise 9.8 SP5 Critical Patch 3 is an integrated security solution for your mobile devices. Read this chapter to understand Mobile Security components, features and how they protect your mobile devices.

This chapter includes the following sections:

- *Understanding Mobile Threats on page 1-2*
- *About Trend Micro Mobile Security on page 1-2*
- *Architecture of Mobile Security System on page 1-3*
- *Components of Mobile Security System on page 1-3*
- *What's New in Release 9.8 SP5 Critical Patch 3 on page 1-6*
- *Main Mobile Device Agent Features on page 1-15*
- *Supported Mobile Device OS Features on page 1-16*

Understanding Mobile Threats

With the standardization of platforms and their increasing connectivity, mobile devices are susceptible to an increasing number of threats. The number of malware programs that run on mobile platforms is growing and more spam messages are sent through SMS. New sources of content, such as WAP and WAP Push are also used to deliver unwanted material.

Additionally, the theft of mobile devices may lead to the compromise of personal or sensitive data.

About Trend Micro Mobile Security

Trend Micro™ Mobile Security for Enterprise is a comprehensive security solution for your mobile devices. Mobile Security incorporates the Trend Micro anti-malware technologies to effectively defend against the latest threats to mobile devices.

The integrated filtering functions enable Mobile Security to block unwanted network communication to mobile devices.

This version of Mobile Security is independent of OfficeScan™ and can be installed separately as a standalone application on a Windows computer.

WARNING!

Trend Micro cannot guarantee compatibility between Mobile Security and file system encryption software. Software products that offer similar features like anti-malware scanning, are may be incompatible with Mobile Security.

About Machine Learning in Trend Micro Mobile Security

Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging unknown security risks through digital DNA fingerprinting, API mapping, and other file features. Predictive Machine

Learning is a powerful tool that helps protect your environment from unidentified threats and zero-day attacks.

After detecting an unknown or low-prevalence file, Mobile Security scans the file using the next generation mobile engine to extract file features and sends the report to the Predictive Machine Learning engine, hosted on the Trend Micro Smart Protection Network. Through use of malware modeling, Predictive Machine Learning compares the sample to the malware model, assigns a probability score, and determines whether the file is malicious or not. Mobile Security can prevent the affected file from installation and remind user to uninstall or remove it.

Architecture of Mobile Security System

Depending on your company needs, you can implement Mobile Security with different client-server communication methods. You can also choose to set up one or any combination of client-server communication methods in your network.

Trend Micro Mobile Security supports three different models of deployment:

- Enhanced Security Model (Dual Server Installation) with Cloud Communication Server
- Enhanced Security Model (Dual Server Installation) with Local Communication Server
- Basic Security Model (Single Server Installation)

Refer to the *Installation and Deployment Guide* for the details.

Components of Mobile Security System

The following table provides the descriptions of the Mobile Security components.

TABLE 1-1. Components of Mobile Security System

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
Management Server	The Management Server enables you to manage Mobile Device Agents from the administration web console. Once mobile devices are enrolled to the server, you can configure Mobile Device Agent policies and perform updates.	Required
Communication Server	The Communication Server handles communications between the Management Server and Mobile Device Agents. Trend Micro Mobile Security provides two types of Communication Server: • Local Communication Server (LCS)—this is a Communication Server deployed locally in your network. • Cloud Communication Server (CCS)—this is a Communication Server deployed in the cloud and you will not need to install this server. Trend Micro manages the Cloud Communication Server and you only need to connect to it from the Management Server. See *Comparison Between Local and Cloud Communication Servers on page 1-6*.	Required
Mobile Device Agent (MDA)	The Mobile Device Agent is installed on the managed Android and iOS mobile devices. The agent communicates with the Mobile Security Communication Server and executes the commands and policy settings on the mobile device.	Required
Microsoft SQL Server	The Microsoft SQL Server hosts the databases for Mobile Security Management Server.	Required
Active Directory	The Mobile Security Management Server imports users and groups from the Active Directory.	Optional

Component	Description	Required or Optional
Certificate Authority	The Certificate Authority manages security credentials and public and private keys for secure communication.	Optional
SCEP	The Simple Certificate Enrollment Protocol (SCEP) is a communication protocol that provides a networked front end to a private certificate authority. In some environments, it is important to make sure that corporate settings and policies are protected from prying eyes. To provide this protection, iOS allows you to encrypt profiles so that they can be read only by a single device. An encrypted profile is just like a normal configuration profile except that the configuration profile payload is encrypted with the public key associated with the device's X.509 identity. The SCEP works with the Certificate Authority to issue certificates in large enterprises. It handles the issuing and revocation of digital certificates. The SCEP and Certificate Authority can be installed on the same server.	Optional
SSL certificate	(**Full Version** deployment mode, and **Security Scan** deployment mode with unlisted MDM vendor only.) Trend Micro Mobile Security requires an SSL server certificate issued from a recognized Public Certificate Authority for the secure communication between mobile devices and Communication Server using HTTPS.	Required, if you want to manage iOS mobile devices
SMTP Server	Connect SMTP server to make sure administrators can get reports from Mobile Security Management Server, and send invitations to users.	Optional

Comparison Between Local and Cloud Communication Servers

The following table provides the comparison between the Local Communication Server (LCS) and the Cloud Communication Server (CCS).

TABLE 1-2. Comparison between Local and Cloud Communication Servers

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

What's New in Release 9.8 SP5 Critical Patch 3

The following new features are available in Trend Micro Mobile Security 9.8 SP5 Critical Patch 3:

FEATURE	DESCRIPTION
Support for Notification Using Firebase Cloud Messaging	This version of Mobile Security uses Google's Firebase Cloud Messaging (FCM) solution to send notifications to Android devices. The FCM solution helps improve the performance and stability of the communication between Mobile Security servers and Android agents.
Bug fix for iOS device locating failure	This version of Mobile Security fixes the issue of occasionally failing to locate iOS devices.

What's New in Release 9.8 SP5 Critical Patch 2

The following new features are available in Trend Micro Mobile Security 9.8 SP5 Critical Patch 2:

Feature	Description
Security Vulnerability Fix	This version of Mobile Security resolves a potential unauthenticated file deletion issue on the Management Server.

What's New in Release 9.8 SP5 Critical Patch 1

The following new features are available in Trend Micro Mobile Security 9.8 SP5 Critical Patch 1:

Feature	Description
Legacy Binary Protocol Replacement	This version of Mobile Security replaces the legacy binary protocol, which will not be supported by Apple from March 31, 2021, with HTTP/2-based Apple Push Notification service (APNs).
Bug Fixes	This version of Mobile Security fixes some known bugs for Android.

What's New in Release 9.8 SP5

The following new features are available in Trend Micro Mobile Security 9.8 SP5:

Feature	Description
MARS Pattern Update from Apex Central	This version of Mobile Security supports MARS pattern update from Trend Micro Apex Central.
PHP Version Upgrade	This version of Mobile Security upgrades the built-in PHP version from 7.0.33 to 7.4.12.

Feature	Description
Support for the Latest Microsoft Exchange Server Version	This version of Mobile Security supports Microsoft Exchange Server 2016/2019.
Support for More Agent Versions	This version of Mobile Security adds support for Android with Server 11.0 and iPadOS 14.

What's New in Release 9.8 SP4

The following new features are available in Trend Micro Mobile Security 9.8 SP5 Critical Patch 3:

Note

Trend Micro Mobile Security certificate is upgraded to help strengthen security. Some services may be affected by the certificate upgrade. You are strongly recommended to upgrade the Trend Micro Mobile Security server to 9.8 SP5 Critical Patch 3 to mitigate the impact of certificate upgrade.

Feature	Description
Integration with Apex Central	This version of Mobile Security updates the policy page in Trend Micro Apex Central.
Support for the Latest iOS Version	This version of Mobile Security adds iOS 14 support.

What's New in Release 9.8 SP3

The following new features are available in Trend Micro Mobile Security 9.8 SP3:

Feature	Description
Integration with Apex Central	This version of Mobile Security integrates with Trend Micro Apex Central to provide central management in Security Scan mode.
Integration with BlackBerry UEM Mobile Device Management Solution	This version of Mobile Security provides security scan for Android and iOS mobile devices while integrating with BlackBerry UEM mobile device management solution.

What's New in Release 9.8 SP2 Patch 1

The following new features are available in Trend Micro Mobile Security 9.8 SP2 Patch 1:

Feature	Description
Android and iOS Compatibility Issue Fix	This version of Mobile Security fixes iOS 13 and Android 10 compatibility issue.
Other Bug Fixes	This version of Mobile Security fixes some other bugs and vulnerability issues in server and mobile device administrators.

What's New in Release 9.8 SP2

The following new features are available in Trend Micro Mobile Security 9.8 SP2:

Feature	Description
Installation of Newer Version of Microsoft SQL Server	This version of Mobile Security installs Microsoft SQL server 2017 during installing.
Replacing JRE with OpenJDK	This version of Mobile Security replaces JRE with OpenJDK to install .apk files on mobile devices.

What's New in Release 9.8 SP1

The following new features are available in Trend Micro Mobile Security 9.8 SP1:

Feature	Description
Support for High Availability for Local Communication Server	Enables you to configure Windows server for High Availability for all Local Communication Servers on the network.
Integration with Citrix XenMobile and IBM MaaS360 Mobile Device Management Solutions	Provides security scan for Android and iOS mobile devices while integrating with Citrix XenMobile and IBM MaaS360 mobile device management solutions.

What's New in Release 9.8

The following new features are available in Trend Micro Mobile Security 9.8:

Feature	Description
Invitation email (Android Only)	Enables administrators to send an invitation email to all users when deploying Mobile Device Agent through AirWatch.
More Security Scans and Detections:	Supports scanning mobile devices for the following: • malicious SSL certificates • malicious iOS profiles (iOS only) • network traffic decryption • unsafe access point (Wi-Fi) • developer options and USB debugging (Android only) • modified applications

Feature	Description
New Widgets, Administrator Notifications, and Reports	Introduces new widgets, administrator notifications and reports for malicious SSL certificate, malicious iOS profile, network traffic decryption, unsafe access point (Wi-Fi), developer options, USB debugging, modified applications, and rooted/jailbroken mobile devices.
Application Approved List	Introduces an approved list for administrators to add the applications that are detected as malware, vulnerable, privacy risk or modified applications, as safe to allow the installation of such applications on mobile devices.
iOS Mobile Device Agent Support	Supports iOS mobile device agent for Security Scan mode with AirWatch and MobileIron only.

What's New in Release 9.7 Patch 3

The following new features are available in Trend Micro Mobile Security 9.7 Patch 3:

Feature	Description
Provides QR Code for Quick Agent Deployment (Security Scan Deployment Mode Only)	Provides enrollment information using QR code on the agent deployment settings screen for quick and simple agent deployment. This feature is only available in Security Scan Deployment Mode with integration with AirWatch and MobileIron.
Supports Predictive Machine Learning	Supports Trend Micro Predictive Machine Learning to perform in-depth file analysis to detect emerging known security risks.

What's New in Release 9.7 Patch 2

The following new features are available in Trend Micro Mobile Security 9.7 Patch 2:

Feature	Description
Integration with MobileIron Mobile Device Management Solutions	Provides security scan for Android and iOS mobile devices while integrating with the following MobileIron mobile device management solutions: • MobileIron Core Hosted • MobileIron Core On-Premise
Integration of Online Help	Links all the UI screens to the help files available on Trend Micro Online Help Center.
Supports iOS Activation Lock (Full Version Deployment Mode Only)	Activation Lock is a feature of Find My iPhone that is built into mobile devices with iOS 7 and later. It prevents reactivation of lost or stolen mobile device by requiring the user's Apple ID and password before anyone can turn off Find My iPhone, erase, or reactivate and use the mobile device.

What's New in Release 9.7

The following new features are available in Trend Micro Mobile Security 9.7:

Feature	Description
Multiple Deployment Modes	Enables you to deploy Trend Micro Mobile Security in: • **Full Version** deployment mode, that includes all the features of Trend Micro Mobile Security. • **Security Only** deployment mode, that provides security scan for Android and iOS mobile devices while integrating with other mobile device management (MDM) solutions.
Integration with AirWatch	Provides security scan for Android and iOS mobile devices while integrating with AirWatch mobile device management solution.
Cyber Security News Widget on Dashboard Screen	Includes a widget on the **Dashboard** screen to display Cyber Security News for mobile devices, published by Trend Micro.

Feature	Description
Server Certificate Verification on Android Devices	Enables you to perform server certificate verification on Android mobile devices.
New MARS API for Security Scanning	Integrates with the latest Mobile Application Reputation Service (MARS) API to enhance the vulnerability detection and description.
Support for Latest Android and iOS Versions	Adds Android 7 and iOS 10 support.

What's New in Release 9.6 SP1

The following new features are available in Trend Micro Mobile Security 9.6 SP1:

Feature	Description
Ransomware Detection Widgets	New widgets on the Dashboard allows administrators to view ransomware detection statistics.
Android App Version Selection	Administrators can choose to deploy the **Full version** or **Security scan only** app for Android and iOS devices.
Automatic App Activation on Android Devices	This version of Mobile Security provides automatic activation on Android devices during app deployment.
Exchange Server Data Cleanup (Full Version Deployment Mode only)	Administrators can perform a data cleanup before transferring to another Exchange server. This allows administrators to remove existing Exchange Connector and Exchange ActiveSync device data on Mobile Security.
Group Setting for Multiple Active Directory Users	Administrators can apply the group setting to multiple Active Directory users.
Report Generation by Device Platform	Enhancements to the report generation feature allow administrators to generate reports for selected device platforms.

Feature	Description
Device Information Update	Administrators can update the device information of a managed mobile device before the next scheduled update.

What's New in Release 9.6

The following new features are available in Trend Micro Mobile Security 9.6:

Feature	Description
User Management	Enables administrators to manage users and invitations separately.
On-Demand Reports	Administrators now have the option of generating reports as needed.
Scheduled Scan	Enables administrators to run the malware and security scans daily, weekly, or monthly based on the specified schedule.
Security Scan for Android	In addition to the privacy scan, Mobile Security now supports the vulnerability scan and modified apps scan for increased security.
New Widgets	This release introduces five new widgets that display information about the Android security scans and the iOS malware scan.
New iOS App Version	Administrators can choose to deploy a new version of the iOS app that only supports security scans and works with 3rd-party mobile device management (MDM) apps.

Main Mobile Device Agent Features

Feature Name	Description		Android	iOS
Security Scanning	Mobile Security incorporates Trend Micro's anti-malware technology to effectively detect threats to prevent attackers from taking advantage of vulnerabilities on mobile devices. Mobile Security is specially designed to scan for mobile threats.	Malware scan	●	●
		Privacy scan	●	
		Vulnerability scan	●	
		Modified Apps scan	●	●
		USB debugging scan	●	
		Developer options scan	●	
		Rooted mobile device scan	●	
		Jailbroken mobile device scan		●
		Malicious iOS profiles scan		●
		Network traffic decryption scan	●	●
		Malicious SSL certificate scan	●	●
		Unsafe access point (Wi-Fi) scan	●	
Authentication	After installing the Mobile Device Agent, the mobile device user need to provide the authentication information to enroll the mobile devices with the Mobile Security Management Server.		●	●

Feature Name	Description		Android	iOS
Regular Updates	To protect against the most current threats, you can either update Mobile Security manually or configure it to update automatically. To save cost, you can also set a different update frequency for the mobile devices that are in “roaming”. Updates include component updates and Mobile Security program patch updates.		●	
Mobile Device Agent Logs	Mobile Device Agent Logs available on Management Server.	Application scan logs	●	●
		Device vulnerability logs	●	●
		Network protection logs	●	●
		Web threat protection logs	●	
	Mobile Device Agent keeps user logs on the mobile device.	Malware scan history	●	
		Vulnerability scan logs	●	
		Modified app scan logs	●	
		Privacy scan history	●	
		Web blocking history	●	

Supported Mobile Device OS Features

The following table shows the list of features that Trend Micro Mobile Security supports on each platform.

TABLE 1-3. Trend Micro Mobile Security 9.8 SP5 Critical Patch 3 Feature Matrix

POLICY	FEATURES	SETTINGS		
Device Security	Security Settings	Real-time scan		●
		Scan after pattern update		●
		Manual scan	●	●
Data Protection	Web Threat Protection	Server-side control		●
		Use blocked list		●
		Use approved list		●
		Allow specific websites only		●
		Allow limited adult content		●

Chapter 2

Getting Started with Mobile Security

This chapter helps you start using Mobile Security and provides you the basic usage instructions. Before you proceed, be sure to install the Management Server, Communication Server, and the Mobile Device Agent on mobile devices.

This chapter includes the following sections:

- *Accessing the Administration Web Console on page 2-2*
- *Dashboard Information on page 2-5*
- *Administration Settings on page 2-9*
- *Command Queue Management on page 2-18*
- *Managing Certificates on page 2-20*

Administration Web Console

You can access the configuration screens through the Mobile Security administration web console.

The web console is the central point for managing and monitoring Mobile Security throughout your corporate network. The console comes with a set of default settings and values that you can configure based on your security requirements and specifications.

You can use the web console to do the following:

- Manage Mobile Device Agents installed on mobile devices
- Configure security policies for Mobile Device Agents
- Configure scan settings on a single or multiple mobile devices
- Group devices into logical groups for easy configuration and management
- View registration and update information

Accessing the Administration Web Console

Procedure

1. Log on to the administration web console using the following URL structure:

   ```
   https://
   <External_domain_name_or_IP_address>:<HTTPS_port>/mdm/web
   ```

   Note

   Replace <External_domain_name_or_IP_address> with the actual IP address, and <HTTPS_port> with the actual port number of the Management Server.

The following screen appears.

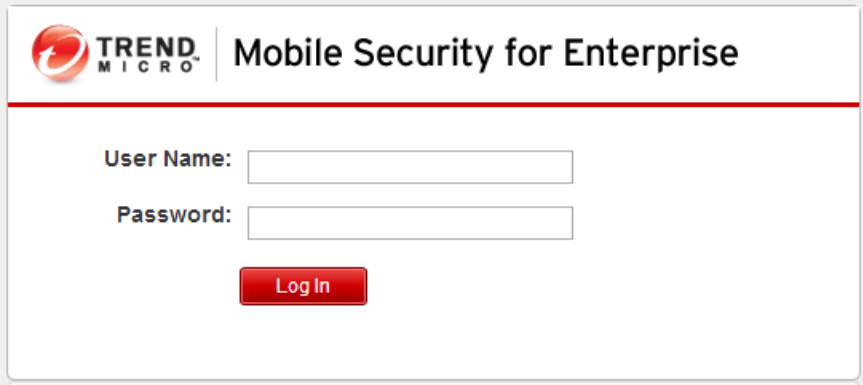


FIGURE 2-1. Administration Web console login screen

2. Type a user name and password in the fields provided and click **Log In**.

Note

The default **User Name** for administration web console is “root” and the **Password** is “mobilesecurity”.

Make sure that you change the administrator password for the user "root" after your first sign in. See “Editing an Administrator Account” in the *Administrator's Guide* for the procedure.

Important

- the **Compatibility View for Websites** options is turned off. See *Turning Off Compatibility Mode in Internet Explorer on page 2-4* for details.
- the JavaScript is enabled on your browser.

Note

If you are unable to access the administration web console in Windows 2012 using Internet Explorer 10 in Metro mode, verify that the **Enhanced Protected Mode** option is disabled in Internet Explorer.

Turning Off Compatibility Mode in Internet Explorer

Trend Micro Mobile Security does not support **Compatibility View** on Internet Explorer. If you are using Internet Explorer to access the Mobile Security administration web console, turn off the web browser's Compatibility View for the website, if it is enabled.

Procedure

1. Open Internet Explorer and click **Tools** > **Compatibility View settings**.

   The **Compatibility View Settings** window displays.

2. If the administration console is added to the **Compatibility View** list, select the website and click **Remove**.

3. Clear **Display intranet sites in Compatibility View** and **Display all websites in Compatibility View** checkboxes, and then click **Close**.

Product License

After the Evaluation version license expires, all program features will be disabled. A Full license version enables you to continue using all features, even after the license expires. It's important to note however, that the Mobile Device Agent will be unable to obtain updates from the server, making anti-malware components susceptible to the latest security risks.

If your license expires, you will need to register the Mobile Security Management Server with a new Activation Code. Consult your local Trend Micro sales representative for more information.

To download updates and allow remote management, Mobile Device Agent must enroll to the Mobile Security Management Server. For instructions to manually enroll Mobile Device Agent on mobile devices, refer to the *Installation And Deployment Guide*.

To view license upgrade instructions for Management Server, click the **View license upgrade instructions** link in Mobile Security **Product License** screen.

Dashboard Information

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 two tabs:

- **Summary**—shows cyber security news related to mobile devices, the mobile device health and security statuses and mobile device operating system version summary.
- **Security**—shows Android device vulnerability scan summary, iOS device vulnerability scan summary, Android network protection summary, iOS network protection summary, Android application risk summary, iOS application risk summary. In this category, you can see the following widgets and statuses:
  - **Android/iOS Vulnerability Summary:**
    - **Rooted**: (Android only) the number of rooted mobile devices
    - **USB Debugging**: (Android only) the number of mobile devices with USB debug mode enabled
    - **Developer Options**: (Android only) the number of mobile devices with developer mode enabled
    - **Jailbroken**: (iOS only) the number of jailbroken mobile devices

- **Malicious iOS Profiles**: (iOS only) the number of mobile devices with installed malicious iOS profiles

- **Android/iOS Network Protection Summary**:
  - **Unsafe Access Point (Wi-Fi)**: (Android only) the number of mobile devices connected to suspicious or unsecured access points (Wi-Fi) with weak or no password
  - **Network Traffic Decryption**: the number of mobile devices detected with decrypted network traffic
  - **Malicious SSL Certificate**: the number of mobile devices with installed malicious SSL certificates
- **Android/iOS Application Risk Summary**:
  - **Malware**: the number of installed applications detected as malware
  - **Vulnerability App**: (Android only) the number of installed applications detected as vulnerable
  - **Privacy Risk**: (Android only) the number of installed applications detected leaking privacy
  - **Modified Apps**: the number of installed applications with modified application package

Customizing the Dashboard

Mobile Security enables you to customize the **Dashboard** information according to your needs and requirements.

Adding a New Tab

Procedure

1. On the **Dashboard** screen, click the + button.

2. On the **New Tab** pop-up window, do the following:
   - **Title**: type the tab name.
   - **Layout**: select the layout for the widgets displayed on the tab.
   - **Auto-fit**: select **On** or **Off** to enable or disable the setting for the widgets on the tab.
3. Click **Save**.

Removing a Tab

Procedure

1. Click the tab, and then click the × button displayed on the tab.
2. Click **OK** on the confirmation pop-up dialog.

Adding Widgets

Procedure

1. On the **Dashboard** screen, click the tab on which you want to add widgets.
2. Click **Add Widgets** on the top-right of the tab.

   The **Add Widgets** screen displays.
3. Select the category from the left menu and/or type the keywords in the search field to display the relevant widgets list.
4. Select the widgets that you want to add, and then click **Add**.

   The selected widgets appear on the tab on the **Dashboard**.

Removing Widgets

Procedure

1. On the **Dashboard** screen, click the tab from which you want to remove widgets.
2. On the widget that you want to remove, click × on the top-right of the widget.

Changing Widget's Position

Procedure

1. On the **Dashboard** screen, click the tab whose widgets you want to rearrange.
2. Click and hold the widget title bar, then drag and drop it to the new position.

Refreshing the Information on the Widgets

Procedure

1. On the **Dashboard** screen, click the tab whose widget you want to refresh.
2. On the widget that you want to refresh, click ⟳ on the top-right of the widget.

Viewing or Modifying Tab Settings

Procedure

1. On the **Dashboard** screen, click the tab whose settings you want to view or modify.
2. Click **Tab Settings**.
3. Modify the settings as required, and then click **Save**.

Administration Settings

Configuring Active Directory (AD) Settings

Trend Micro Mobile Security enables you to configure user authorization based on the Active Directory (AD). You can also add mobile devices to the device list using your AD. Refer to the *Initial Server Setup* section in the *Installation and Deployment Guide* for the detailed configuration steps.

Configuring User Authentication

Trend Micro Mobile Security enables you to configure user authentication based on the Active Directory (AD) or through an Enrollment Key. Refer to the *Initial Server Setup* section in the *Installation and Deployment Guide* for the detailed configuration steps.

Configuring Database Settings

Refer to the *Initial Server Setup* section in the *Installation and Deployment Guide* for the detailed configuration steps.

Configuring Communication Server Settings

Refer to the *Initial Server Setup* section in the *Installation and Deployment Guide* for the detailed configuration steps.

Configuring Deployment Settings

Refer to the *Initial Server Setup* section in the *Installation and Deployment Guide* for the detailed configuration steps.

Switching from Full Version to Security Scan Deployment Mode

You can switch the deployment mode for Mobile Security at anytime.

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

https://success.trendmicro.com/solution/1115884

Configuring AirWatch Integration with Trend Micro Mobile Security

Trend Micro Mobile Security enables you to integrate with AirWatch device management solution.

Refer to the topic *Integration with AirWatch* in *Chapter 3, Integration with Other MDM Solutions* in *Administrator's Guide for Security Only Deployment Mode* for the details.

Configuring MobileIron Integration with Trend Micro Mobile Security

Trend Micro Mobile Security enables you to integrate with MobileIron device management solution.

Refer to the topic *Integration with MobileIron* in *Chapter 3, Integration with Other MDM Solutions* in *Administrator's Guide for Security Only Deployment Mode* for the details.

Configuring Citrix XenMobile Integration with Trend Micro Mobile Security

Trend Micro Mobile Security enables you to integrate with Citrix XenMobile device management solution.

Refer to the topic *Integration with Citrix XenMobile* in *Chapter 3, Integration with Other MDM Solutions* in *Administrator's Guide for Security Only Deployment Mode* for the details.

Configuring IBM MaaS360 Integration with Trend Micro Mobile Security

Trend Micro Mobile Security enables you to integrate with IBM MaaS360 device management solution.

Refer to the topic *Integration with IBM MaaS360* in *Chapter 3, Integration with Other MDM Solutions* in *Administrator's Guide for Security Only Deployment Mode* for the details.

Managing Administrator Accounts

The **Administrator Account Management** screen enables you to create user accounts with different access role for the Management Server.

Default Administrator Account Name and Role

The default administrator account is “root” (password: “mobilesecurity”). The root account cannot be deleted and can only be modified. See *Editing an Administrator Account on page 2-15* for the detailed procedure.

TABLE 2-1. The root account properties

ROOT ACCOUNT PROPERTIES		CAN BE MODIFIED?
Administrator Accounts	Account name	No
	Full name	Yes
	Password	Yes
	Email address	Yes
	Mobile phone number	Yes
Administrator Roles	Administrator role modification	No

The default administrator role is **Super Administrator**, which has the maximum access to all settings. The **Super Administrator** role cannot be deleted and can only be modified. See *Editing an Administrator Role on page 2-17* for the detailed procedure.

TABLE 2-2. The Super Administrator role properties

SUPER ADMINISTRATOR ROLE PROPERTIES		CAN BE MODIFIED?
Role Details	Administrator role	No
	Description	Yes
Group Management Control	Managed Groups	No

TABLE 2-3. Access rights for Super Administrator and a Group Administrator

SERVER COMPONENTS	PERMISSIONS	SUPER ADMINISTRATOR	GROUP ADMINISTRATOR
Administration	Updates	Supported	Not supported
	Administrator Account Management	Can modify all the account	Can only modify own account information
	Device Enrollment Settings	Supported	Not supported
	Certificate Management	Supported	Supported
	Command Queue Management	Can manage all commands	Can only view commands for the related groups
	Database Settings	Supported	Not supported
	Communication Server Settings	Supported	Not supported
	Active Directory Settings	Supported	Not supported
	Management Server Settings	Supported	Not supported
	Deployment Settings	Supported	Not supported
	Configuration and Verification	Supported	Not supported
	Product License	Supported	Not supported
Notifications/ Reports	Log Query	All the groups	Managed groups only
	Log Maintenance	All the groups	Managed groups only
	Administrator Notifications/Reports	Supported	Not supported
	User Notifications	Supported	Not supported
	Settings	Supported	Not supported

Server Components	Permissions	Super Administrator	Group Administrator
Applications		Supported	Supported for managed groups only
Policy	Create a policy	Supported	Supported for managed groups only
	View a policy	Supported	Supported for managed groups only
	Copy a policy	Supported	Supported for managed groups only
	Delete a policy	Supported	Supported for managed groups only
Devices	View devices	Supported	Supported for managed groups only
	Add group	Supported	Supported
Users	Invite users	Supported	Supported for managed groups only

Adding Administrator Accounts

Procedure

1. On the Mobile Security administration web console, go to **Administration** > **Administrator Account Management**.
2. On the **Administrator Accounts** tab, click **Create** to add a new account.

   The **Create Administrator Account** screen appears.
3. Under section **Account Details**, do one of the following:
   - Select **Trend Micro Mobile Security User**, and specify the following user account details:

- **Account name**: name used to log on to the Management Server.
- **Full name**: the user's full name.
- **Password** (and **Confirm Password**).
- **Email address**: the user's email address.
- **Mobile phone number**: the user's phone number.

- Select **Active Directory user**, and do the following:

  a. Type the user name in the search field and click **Search**.

  b. Select the user name from the list on the left and click **>** to move the user to the **Selected users** list on the right.

Note

To remove the user from the **Selected users** list on the right, select the user name and click **<**.

You can also select multiple users at the same time by holding Ctrl or Shift keys while clicking on the username.

4. Under section **Administrator Role**, select the role from the **Choose the administrator role:** drop-down list.

   See *Creating an Administrator Role on page 2-17* for the procedure for creating administrator roles

5. Click **Save**.

Editing an Administrator Account

Procedure

1. On the Mobile Security administration web console, go to **Administration** > **Administrator Account Management**.
2. On the **Administrator Accounts** tab, click **Create** to add a new account.

The **Edit Administrator Account** screen appears.

3. Modify the administrator account details and access role as required.
   - Account Details
     - **Account name**: name used to log on to the Management Server.
     - **Full name**: the user's full name.
     - **Email address**: the user's email address.
     - **Mobile phone number**: the user's phone number.
     - **Password**: click **Reset Password** to change the user account password, type the new password in the **New Password** and **Confirm Password** fields, and click **Save**.
   - **Administrator Role**
     - **Choose the administrator role**: select the administrator role from the drop-down list.

       For the procedure to create an administrator role, see *Creating an Administrator Role on page 2-17*.
4. Click **Save**.

Deleting an Administrator Account

Procedure

1. On the Mobile Security administration web console, go to **Administration** > **Administrator Account Management**.
2. On the **Administrator Accounts** tab, select the administrator accounts that you want to delete, and then click **Delete**.

   A confirmation message appears.

Creating an Administrator Role

Procedure

1. On the Mobile Security administration web console, go to **Administration** > **Administrator Account Management**.
2. On the **Administrator Roles** tab, click **Create**.

   The **Create Administrator Role** screen appears.
3. Under section **Role Details**, provide the following information:
   - Administrator Role
   - Description
4. Under section **Group Management Control** select the mobile device groups that this administrator role can manage.
5. Click **Save**

Editing an Administrator Role

Procedure

1. On the Mobile Security administration web console, go to **Administration** > **Administrator Account Management**.
2. On the **Administrator Roles** tab, click **Create**.

   The **Create Administrator Role** screen appears.
3. Modify the role details as required and then click **Save**.

Deleting an Administrator Role

Procedure

1. On the Mobile Security administration web console, go to **Administration** > **Administrator Account Management**.
2.
3. On the **Administrator Roles** tab, select the administrator role you want to delete, and click **Delete**.

   A confirmation message appears.

Changing Administrator Password

Refer to the topic *Editing an Administrator Account on page 2-15* for the procedure of changing the administrator account password.

Command Queue Management

Mobile Security keeps a record of all the commands you have executed from the web console and enables you to cancel or resend a command, if required. You can also remove the commands that have already been executed and are not required to be displayed on the list.

To access the **Command Queue Management** screen, go to **Administration** > **Command Queue Management**.

The following table describes all the command statuses on the **Command Queue Management** screen.

Command Status	Description
Waiting to Send	The Mobile Security Management Server is in the process of sending the command to mobile device. You can cancel the command while it is in this status.
Waiting Acknowledgment	The Mobile Security Management Server has sent the command to mobile device and is waiting for the acknowledgement from the mobile device.
Unsuccessful	Unable to execute the command on mobile device.
Successful	The command has been executed successfully on the mobile device.
Canceled	The command has been canceled before it was executed on the mobile device.

To keep the size of commands from occupying too much space on your hard disk, delete the commands manually or configure Mobile Security administration web console to delete the commands automatically based on a schedule in the **Command Queue Maintenance** screen.

Configuring Schedule for Deleting Old Commands

Procedure

1. Click **Administration** > **Command Queue Management**.

   The **Command Queue Management** screen displays.

2. On the **Command Queue Maintenance** tab, select **Enable scheduled deletion of commands**.

3. Specify the number of days old commands you want to delete.

4. Specify the commands queue deletion frequency and time.

5. Click **Save**.

Deleting Old Commands Manually

Procedure

1. Click **Administration** > **Command Queue Management**.

   The **Command Queue Management** screen displays.

2. On the **Command Queue Maintenance** tab, select **Enable scheduled deletion of commands**.

3. Specify the number of days old commands you want to delete.

4. Click **Delete Now**.

Managing Certificates

Use the **Certificate Management** screen to upload `.pfx`, `.p12`, `.cer`, `.crt`, `.der` certificates to the Mobile Security Management Server.

Uploading a Certificate

Procedure

1. Log on to the Mobile Security administration web console.

2. Click **Administration** > **Certificate Management**.

3. Click **Add**.

   The **Add certificate** window appears.

4. Click **Choose File** and then select a `.pfx`, `.p12`, `.cer`, `.crt`, `.der` certificate file.

5. Type the certificate password in the **Password** field.

6. Click **Save**.

Deleting a Certificate

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Administration** > **Certificate Management**.
3. Select the certificates that you want to delete, and then click **Delete**.

Chapter 3

Integrating with Other MDM Solutions

Trend MicroMobile Security enables you to integrate other mobile device management solutions with Mobile Security.

This chapter explains you the procedure to set up Mobile Security integration with other mobile device management solutions.

Topics included in this chapter:

- *Feature Integration Comparison for MDM Solutions on page 3-2*
- *Integration with AirWatch on page 3-3*
- *Integration with MobileIron on page 3-17*
- *Integration with Citrix XenMobile on page 3-25*
- *Integration with IBM MaaS360 on page 3-34*
- *Integration with BlackBerry UEM on page 3-41*

Feature Integration Comparison for MDM Solutions

Trend Micro Mobile Security provides integration with other Mobile Device Management (MDM) solutions. The following table lists the features that are currently supported for each MDM solution.

TABLE 3-1. Feature Integration Comparison for MDM Solutions

FEATURES	AIRWATCH	MOBILEIRON CORE	IBM MAAS360	CITRIX XENMOBILE	BLACKBERRY UEM
Customized Device Security Attribute	Yes (Tag)	Yes	Yes	Yes	
Device Groups Based on Customized Device Security Attribute	Yes (Smart Group)	Yes (Label)	Yes		
Customized Application Groups	Yes (Blacklist)				
Enrollment Configuration of Mobile Security iOS Agent	Yes	Yes	Yes	Yes	Yes
Auto Enrollment of Mobile Security Android Agent	Yes	Yes	Yes	Yes	Yes
Auto Deployment of Mobile Security Android Agent	Yes (Samsung)				
Auto Launch of Mobile Security Android Agent	Yes				

Integration with AirWatch

Trend Micro Mobile Security enables you to integrate AirWatch MDM solution with Mobile Security.

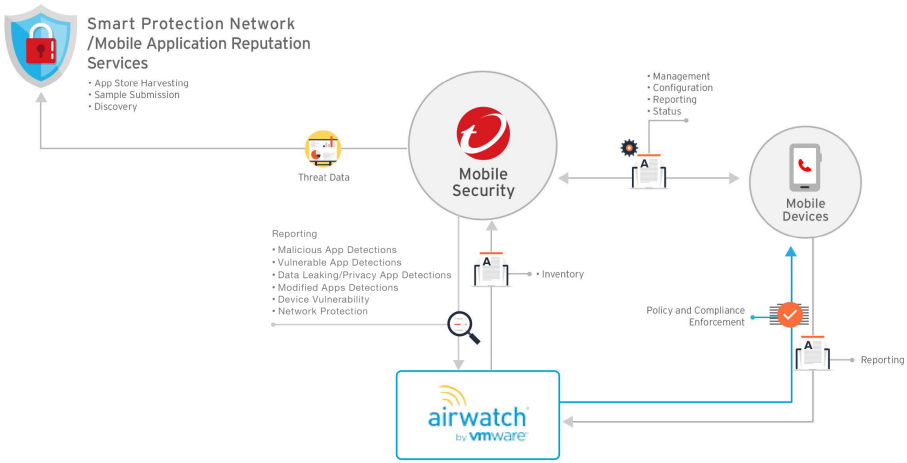
Prerequisites for Integration

To integrate other MDM solutions with Trend MicroMobile Security, you must use the following:

- Mobile Security for Enterprise 9.7 or later
- Local Communication Server or Cloud Communication Server configured in Mobile Security
- AirWatch v9.1 or later
- Admin account on AirWatch administration web console

AirWatch Integration Architecture

The following image shows the high-level architecture of integration with AirWatch.



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. It is the world's first automatic mobile app evaluation service.

The **Trend Micro Smart Protection Network** delivers proactive global threat intelligence against zero-hour threats to ensure that you are always protected. Trend Micro uses the up-to-the-second threat intelligence to immediately stamp out attacks before they can harm you. The **Smart Protection Network** is powering all of Trend Micro products and services.

Mobile Security uses Smart Protection Network and Mobile Application Reputation Services to find mobile device security issues and leverages AirWatch compliance policy to manage your mobile device.

Integration Features

Trend MicroMobile Security provides the following features with integration with AirWatch:

Feature	Description
Automatic Grouping for Mobile Devices	Mobile Security adds Dangerous, Risky, No_TMMS suffixes to tag the mobile devises based on their risk levels. See *Automatic Grouping for Mobile Devices on page 3-5* for details.
Automatic Grouping for Applications	Mobile Security adds Malware, Vulnerability and Privacy prefixes to group the mobile applications based on their risk levels. See *Automatic Grouping for Mobile Applications on page 3-6* for details.

Feature	Description
Automatically Updating AirWatch Blacklist for Policy Violating Apps	This feature enables you to put the apps into the blacklist that violate AirWatch compliance policy (based on the security scan result), and sends an email alert to the user. See *Configuring AirWatch Blacklist Compliance Policy for Apps on page 3-6* for details.
Automatic Deployment of Mobile Security Client App	You can configure AirWatch to automatically deploy mobile device agent to mobile devices. • **Android**: See *Deploying Android Agent Through Mobile Security Server on page 3-13* for the procedure. You can also configure Samsung mobile devices to automatically launch mobile device agent on mobile devices. See *Configuring Automatic Launch for Android Mobile Devices on page 3-14* for the details and procedure. • **iOS**: See *Deploying iOS Agent on page 3-15* for the procedure.

Automatic Grouping for Mobile Devices

Mobile Security uses prefixes to create three (3) classes (Dangerous, Risky and NO_TMMS), and tags the risk devices as follows:

- PREDEFINEDPREFIX_Dangerous
- PREDEFINEDPREFIX _Risky
- PREDEFINEDPREFIX _NO_TMMS

Mobile Security enables you to define prefixes (PREDEFINEDPREFIX) on the administration web console. If Mobile Security detects a mobile device with different security levels, it automatically changes the device's Smart Group.

For example, if Mobile Security detects that a malware on a mobile device, it automatically moves the mobile device to PREDEFINEDPREFIX _Dangerous group.

Automatic Grouping for Mobile Applications

Mobile Security automatically groups the risky applications together under App Groups, based on the type of risk they pose.

- PREDEFINEDPREFIX _Malware_App_Android
- PREDEFINEDPREFIX _Privacy_App_Android
- PREDEFINEDPREFIX _Vulnerability_App_Android
- PREDEFINEDPREFIX _Malware_App_iOS

Mobile Security enables you to define prefixes (PREDEFINEDPREFIX) on the administration web console.

Configuring AirWatch Blacklist Compliance Policy for Apps

After you have configured AirWatch integration settings, you can create compliance policy on AirWatch administration web console to add malicious apps to AirWatch **Blacklist**.

Procedure

1. Log on to the AirWatch web console, and navigate to **Devices** > **Compliance Policies** > **List View**.
2. Click **Add**, select the platform (Android or Apple iOS), and then from the drop-down lists, select **Application List**, and **Contains Blacklisted App(s)**.
3. Click **Next**.
4. On **Actions** tab, configure actions:
   a. Select **Mark as Not Compliant**.
   b. Select **Notify** and **Send Email to User** form the drop-down lists.
   c. Click **Next**.

5. On the **Assignment** tab, configure the following:
   - **Managed By**: `Trend Micro`
   - **Assigned Groups**
   - **Exclusions**
6. Click **Next**.
7. On **Summary** tab, configure the name and description.
8. Click **Finish and Activate**.

On detecting a malware on the mobile device, Mobile Security puts the application into AirWatch blacklist, and the mobile device will be flagged as uncompliant.

AirWatch Account Permission Requirements for Integration

Mobile Security supports the integration with AirWatch. To integrate Mobile Security with AirWatch, you need to have an AirWatch account with required permissions for the communication between the Mobile Security server and AirWatch.

You can create account on AirWatch with three different permission options:

- **Option 1: Create an AirWatch Administrator account for the communication with all permissions**

  On the AirWatch administration console, navigate to **Accounts** > **Administrators** > **List View** > **Add** > **Add Admin**, and create account with the following role and permissions:

  ```
  AirWatch Administrator
  AirWatch Admins (Internal or External) Access to all except
  "dangerous" console features.
  ```

- **Option 2: Create a user with API ONLY with all REST API permissions**

On the AirWatch administration console, navigate to **Accounts** > **Administrators** > **List View** > **Add** > **Add Admin**, and create account with the following role and permissions:

```
API Only
Only provides access to REST APIs
```

- **Option 3: Create a user with API ONLY with customized REST API permissions**

  This option allows you to select the specific REST APIs that Mobile Security uses.

  Do the following:

  1. On the AirWatch administration console, navigate to **Accounts** > **Administrators** > **Roles**, and create a role with the specific REST APIs permissions that Mobile Security uses, as shown in the following table:

CATEGORY	NAME
Admin User Management	Search Admin User
WTag Management	Create Tag
	Search Tag
	Add Devices to the Tag
	Remove Devices from Tag
	Retrieve Devices with Specific Tag
Smart Group Management	Create Smart Group
	Search Smart Groups
	Delete Smart Groups

Category	Name
Application Group Management	Create Application Group
	Search Application Group
	Retrieve Application Group Details
	Add Application to an Application Group
	Delete Application from the Application Group
Application Management	Internal Application Install : Upload Application Chunks (iOS and Android)
	Internal Application Install : Begin Internal Application Install
Device Management	Retrieve Device Information
	Device Extensive Search
	Device Count Info

2. Navigate to **Accounts** > **Administrators** > **List View** > **Add** > **Add Admin**, and add an account with the newly created role.

Note

The AirWatch REST permission settings page does not have permission for each API, but provides a lot of API series (such as, Admin API, APPs API, etc.). Contact AirWatch technical support to know which REST API permissions need to be enabled on the settings page.

Configuring AirWatch Integration

Procedure

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.

3. Click **Administration** > **Deployment Settings**.
4. Under **Server** section, select **Security Scan**, and then select **AirWatch** MDM Solution from the drop down list.
5. Under section **Service Registration**, configure AirWatch settings.
6. Click **Verify Settings** to make sure Mobile Security can connect to the AirWatch server.
7. Under **Data Synchronization Settings** section, configure the following:
   - **Security Category Prefix**

     Note

     Mobile Security uses a prefix to create three (3) classes (Dangerous, Risky and NO_TMMS), and tags the risk devices as follows:

     - XXXX_Dangerous
     - XXXX_Risky
     - XXXX_NO_TMMS

     The risk devices and apps are grouped together under **Smart Groups** and **App Groups** respectively, and includes apps with tag and category added as prefix to their names.

     - Smart Groups: XXXX_Dangerous, XXXX_Risky, XXXX_NO_TMMS.
     - App Groups: XXXX_Malware_App_Android, XXXX_Privacy_App_Android, XXXX_Vulnerability_App_Android, XXXX_Malware_App_iOS
8. Under **Notification Setting** section, select **Automatically send invitation email to user** to send an email notification automatically to the user whenever a new user is synchronized from AirWatch server.

Agent Deployment

Trend Micro Mobile Security enables you to deploy client agent from the two different sources:

- **Google Play Store**: You will need to configure AirWatch to deploy the mobile device agent and provide the enrollment information to users, in the form of text or a QR-code. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen.

  After installing the mobile device agent, users will be required to enroll to the Mobile Security server manually. If you deploy mobile device agent from Google Play Store, the mobile device users can receive the real-time updates via Google Play.

- **Mobile Security Server**: Notify users to download the mobile device agent, with the name: **ENT Security**, from AirWatch app store.

  If you use this deployment option, you will need to provide the enrollment information to users, in the form of text or a QR-code. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen. Whenever a user launches the mobile device agent, the user will need to enroll the app to the Mobile Security server. You can also configure the app to enroll automatically. However, whenever there is an update available, the mobile device users will be required to update their mobile device agents manually.

  On Samsung mobile devices, the AirWatch administration console enables you to deploy and configure the mobile device agent automatically.

Deploying Android Agent Through Google Play Store

Procedure

1. Log on to AirWatch web console, and navigate to **Apps & Books** > **List View** > **Public (tab)** > **ADD APPLICATION**.
2. On the **Add Application** screen, configure the following fields:
   - **Managed By**: Type `Trend Micro`.
   - **Platform**: Select **Android** from the drop-down list.
   - **Source**: Select **Search App Store**.
   - **Name**: Type `ent security` to search the app store.
3. Click **Next**.
4. From the search results, select **Enterprise Mobile Security**.
5. On the **Add Application** screen, click the **Assignment** tab, and select the assigned groups from the **Assigned Groups** field.
6. Click **Save & Publish**.
7. Click **Upload**.

Mobile Security repacks the Android agent with the enrollment key, and uploads it to the server. If there is no preset enrollment key configured, Mobile Security generates an enrollment key before repacking the Android agent.

Note

For Samsung mobile devices, you can also configure the auto-launch function of Mobile Security Android agent on AirWatch web console. Refer to the following article for the details:

https://success.trendmicro.com/solution/1115842

What to do next

If you did not select the **Auto Enrollment** setting, provide the enrollment information to users, in the form of text or a QR-code after deploying the Android agent. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen.

Deploying Android Agent Through Mobile Security Server

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Administration** > **Device Enrollment Settings** on the menu bar.
3. On the **Authentication** tab, select **Authenticate using Enrollment Key**, and then select **Use preset Enrollment Key**.
4. Click **Administration** > **Deployment Settings** > **Android Agent (tab)**.
5. Select **Download from TMMS Server**, and then select **Auto Enrollment**.
6. Click **Save** to save the settings.
7. Click **Upload**, and then select the modified Mobile Security agent file to upload it to the AirWatch server.

   The mobile device agent uploads and appears on the AirWatch administration web console.

What to do next

If you did not select the **Auto Enrollment** setting, provide the enrollment information to users, in the form of text or a QR-code after deploying the Android agent. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen.

Configuring Automatic Launch for Android Mobile Devices

Before you begin

Before performing this procedure, you must perform all the steps as explained in *Deploying Android Agent Through Mobile Security Server on page 3-13*.

Procedure

1. Log on to AirWatch web console, and navigate to **Devices** > **Staging & Provisioning** > **Components** > **Files/Actions**.
2. Configure **Files/Actions** from the AirWatch console. Do the following:
   a. Navigate to **Devices** > **Staging & Provisioning** > **Components** > **Files/Actions**.
   b. • Click **Add** > **Android**.
   c. On the **General** tab, provide the information for the **Name** and **Description** fields.
   d. On the **Manifest** tab, click **Add Action**, located under the **Install Manifest** section.
   e. On the **Add Manifest** options, configure the following information, then click **Save**:
      - **Action(s) to Perform**: Run Intent
      - **Command Line and Arguments to run**:

        ```
        mode=explicit,broadcast=false,action=android.intent.action.MAIN,package=com.trendmicro.tmmssuite.enterprise,class=com.trendmicro.tmmssuite.enterprise.ui.TmmsEnterpriseSplashScreen
        ```

      - TimeOut: [any duration as per your requirements]
   f. On the **Add Files/Actions** screen, click **Save**.

3. Configuring the Product. Do the following:
   a. Navigate to **Devices** > **Staging & Provisioning** > **Product List View**.
   b. • Click **Add Product** > **Android**.
   c. On the **General** tab, provide the information for the **Name**, **Description**, and **Assigned Groups** fields.
   d. On the **Manifest** tab, click **Add** to add the manifest.
   e. On the **Add Manifest** options, configure the following information, then click **Save**:
      - **Action(s) to Perform**: Install Files/Actions
      - **Files/Actions**:

        `TestLauncher`
   f. On the **Add Product** screen, click **Save**.
4. Configuring the Application. Perform the following steps:
   a. Assign the TMMS Agent to a smart group.
   b. Set the **Push Mode** to **Auto**.

Deploying iOS Agent

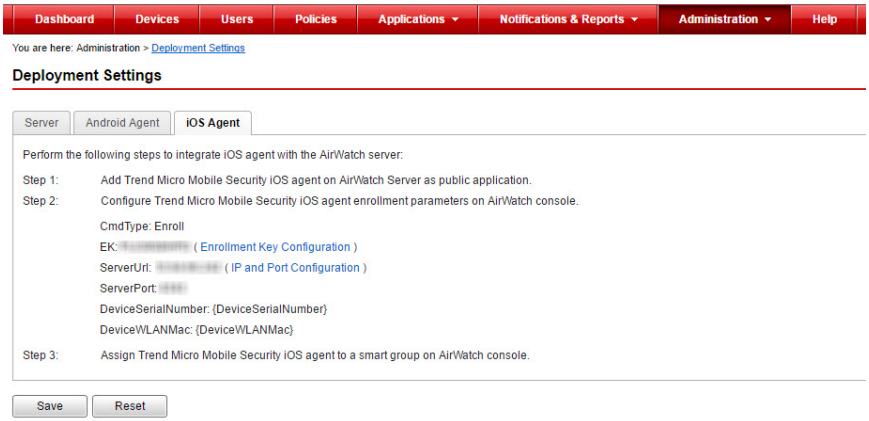
Procedure

1. Log on to the AirWatch web console, and navigate to **Apps & Books** > **Applications** > **List View**.
2. On the **Public** tab, click **ADD APPLICATION**.
3. On the **Add Application** screen, configure the following fields:
   - **Managed By**: Type `Trend Micro`.
   - **Platform**: Select **Apple iOS**.

- **Source**: Select **Search App Store**.
- **Name**: Type **ENT Security**

4. Click **Next**.
5. From the search results, click **Select** before **Mobile Security for Enterprise Agent**.
6. On the **Deployment** tab, select **Send Application Configuration**, and then configure the application under the **Application Configuration** field.

   For application configuration values, refer to **Mobile Security web console** > **Administration** > **Deployment Settings** > **iOS Agent (tab)**.



Configuration Key	Value Type	Configuration Value
CmdType	String	Enroll
EK	String	<Enrollment Key>
ServerUrl	String	<Actual server URL>
ServerPort	String	<Actual server port number>
DeviceSerialNumber	String	{DeviceSerialNumber}

Configuration Key	Value Type	Configuration Value
DeviceWLANMac	String	{DeviceWLANMac}

7. Click **Save & Publish**.
8. On the **View Device Assignment** screen, click **Publish**.

Integration with MobileIron

Trend Micro Mobile Security enables you to integrate the following MobileIron MDM solutions with Mobile Security:

- MobileIron Core Hosted
- MobileIron Core On-premise

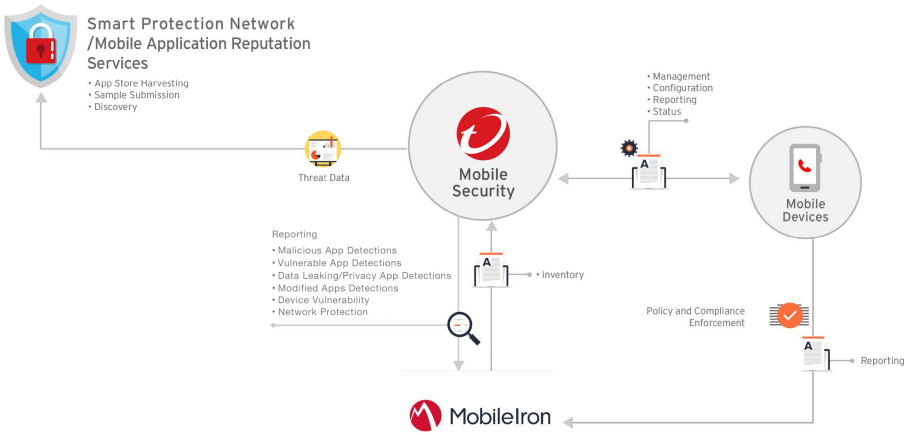
Prerequisites for Integration

To integrate other MDM solutions with Trend MicroMobile Security, you must use the following:

- Mobile Security for Enterprise 9.8 or later
- Local Communication Server or Cloud Communication Server configured in Mobile Security
- MobileIron v9.3 or later
- Admin account on MobileIron administration web console

MobileIron Integration Architecture

The following image shows the high-level architecture of integration with MobileIron.



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. It is the world's first automatic mobile app evaluation service.

The **Trend Micro Smart Protection Network** delivers proactive global threat intelligence against zero-hour threats to ensure that you are always protected. Trend Micro uses the up-to-the-second threat intelligence to immediately stamp out attacks before they can harm you. The **Smart Protection Network** is powering all of Trend Micro products and services.

Mobile Security uses Smart Protection Network and Mobile Application Reputation Services to find mobile device security issues and leverages MobileIron compliance policy to manage your mobile device.

Integration Features

Trend MicroMobile Security provides the following features with integration with AirWatch:

Feature	Description
Automatic Grouping for Mobile Devices	Mobile Security adds Dangerous, Risky and NO_TMMS suffixes to label the mobile devises based on their risk levels. See *Automatic Grouping for Mobile Devices on page 3-19* for details.
Automatic Deployment of Mobile Security Client App	You can configure MobileIron to automatically deploy mobile device agent to mobile devices. • **Android**: See *Deploying Android Agent Through Mobile Security Server on page 3-22* for the procedure. • **iOS**: See *Deploying iOS Agent on page 3-23* for the procedure.

Automatic Grouping for Mobile Devices

Mobile Security uses prefixes to create three (3) classes (Dangerous, Risky and NO_TMMS), and label the risk devices as follows:

- PREDEFINEDPREFIX_Dangerous
- PREDEFINEDPREFIX _Risky
- PREDEFINEDPREFIX _NO_TMMS

Mobile Security enables you to define prefixes (PREDEFINEDPREFIX) on the administration web console. If Mobile Security detects a malicious application, it automatically changes the device's Smart Group.

For example, if Mobile Security detects that a malware on a mobile device, it automatically moves the mobile device to PREDEFINEDPREFIX _Dangerous group.

Configuring MobileIron Integration

Procedure

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.
3. Click **Administration** > **Deployment Settings**.
4. Under **Server** section, select **Security Scan**, and then select **MobileIron Core Hosted**or **MobileIron Core On-Premise** MDM Solution from the drop down list.
5. Under section **Service Registration**, configure MobileIron settings.
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**

     Note

     Mobile Security uses a prefix to create three (3) classes (Dangerous, Risky and NO_TMMS), and labels the risk devices as follows:

     - XXXX_Dangerous
     - XXXX_Risky
     - XXXX_NO_TMMS

Agent Deployment

Trend Micro Mobile Security enables you to deploy client agent from the two different sources:

- **Google Play Store**: You will need to configure MobileIron to deploy the mobile device agent and provide the enrollment information to users, in the form of text or a QR-code. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen.

  After installing the mobile device agent, users will be required to enroll to the Mobile Security server manually. If you deploy mobile device agent from Google Play Store, the mobile device users can receive the real-time updates via Google Play.

- **Mobile Security Server**: Notify users to download the mobile device agent, with the name: **ENT Security**, from MobileIron app store.

  If you use this deployment option, you will need to provide the enrollment information to users, in the form of text or a QR-code. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen. Whenever a user launches the mobile device agent, the user will need to enroll the app to the Mobile Security server. You can also configure the app to enroll automatically. However, whenever there is an update available, the mobile device users will be required to update their mobile device agents manually.

Deploying Android Agent Through Google Play Store

Procedure

1. Log on to MobileIron web console, and click **App Catalog** on the menu bar.

2. Click **Add+**, and then select **Google Play**.
3. In the **Application Name** field, type `ENT Security` , and click **Search**.
4. From the search results, select **Enterprise Mobile Security**, and click **Next**.
5. Add the description for **Enterprise Mobile Security**, and from the **Category** drop-down list, select the category where you want to place this application.
6. Click **Finish**.
7. Click **Apps@Work** form the menu bar.
8. Under the **APPS@WORK CATALOG**, section, select **Feature this App in the Apps@Work catalog**.
9. Click **Save**.

What to do next

If you did not select the **Auto Enrollment** setting, provide the enrollment information to users, in the form of text or a QR-code after deploying the Android agent. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen.

Deploying Android Agent Through Mobile Security Server

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Administration** > **Device Enrollment Settings** on the menu bar.
3. On the **Authentication** tab, select **Authenticate using Enrollment Key**, and then select **Use preset Enrollment Key**.

4. Click **Administration** > **Deployment Settings** > **Android Agent (tab)**.
5. Select **Download from TMMS Server**, and then select **Auto Enrollment**.
6. Click **Save** to save the settings.
7. Click **Upload**, and then select the modified Mobile Security agent file to upload it to the AirWatch server.

   The mobile device agent uploads and appears on the AirWatch administration web console.

What to do next

If you did not select the **Auto Enrollment** setting, provide the enrollment information to users, in the form of text or a QR-code after deploying the Android agent. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen.

Deploying iOS Agent

Procedure

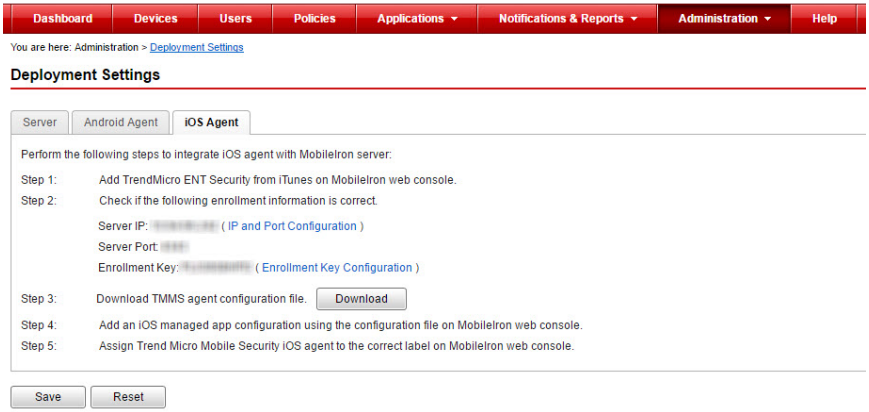
1. Log on to the MobileIron web console, and click **App Catalog**.
2. Click **Add+**, and then select **iTunes**.
3. Type `ENT Security` in the search field, and then click **Search**.
4. Select **Mobile Security for Enterprise Agent**, and click **Next**.
5. Without changing the information, click **Next**.
6. Under **APPS@WORK CATALOG** section, select **Feature this App in the Apps@Work catalog**, and click **Next**.
7. Click **Finish**.
8. Log on to the Mobile Security administration web console.

9. Click **Administration** > **Deployment Settings** > **iOS Agent (tab)**.

10. Click **Download** to download the configuration file.

Note

If the **Download** button is inactive, make sure you have correctly configured all the settings in the previous steps.



11. On the MobileIron administration web console, navigate to **Policies & Configures**.

12. Click **Add New** > **iOS and OS X** > **Managed App Config**

13. Type the following information:

    - **Name**
    - **Description**
    - **BundleId**

14. Click **Download** to download the configuration file.

15. Select the newly created configuration file and then click **More Action** > **Apply to Label**.

16. Click **Apply**.

    Mobile Security pushes the **App Installation** notification to iOS mobile devices.

Integration with Citrix XenMobile

Trend Micro Mobile Security enables you to integrate Citrix XenMobile MDM solution with Mobile Security.

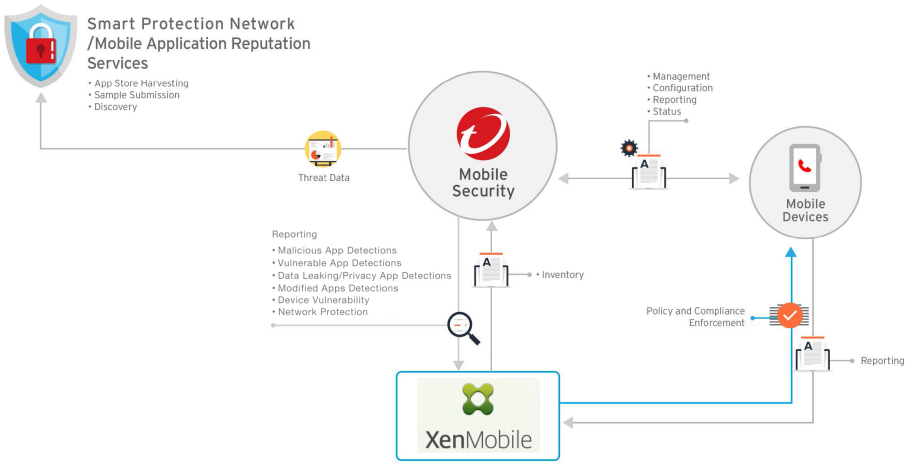
Prerequisites for Integration

To integrate other MDM solutions with Trend MicroMobile Security, you must use the following:

- Mobile Security for Enterprise 9.8 SP5 Critical Patch 3 or later
- Local Communication Server or Cloud Communication Server configured in Mobile Security

Citrix XenMobile Integration Architecture

The following image shows the high-level architecture of integration with Citrix XenMobile.



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. It is the world's first automatic mobile app evaluation service.

The **Trend Micro Smart Protection Network** delivers proactive global threat intelligence against zero-hour threats to ensure that you are always protected. Trend Micro uses the up-to-the-second threat intelligence to immediately stamp out attacks before they can harm you. The **Smart Protection Network** is powering all of Trend Micro products and services.

Mobile Security uses Smart Protection Network and Mobile Application Reputation Services to find mobile device security issues and leverages Citrix XenMobile compliance policy to manage your mobile device.

Integration Features

Trend MicroMobile Security provides the following features with integration with Citrix XenMobile:

Feature	Description
Automatic Grouping for Mobile Devices	Mobile Security adds Dangerous, At Risk, Never Scanned and Protected suffixes to tag the mobile devises based on their risk levels. See *Automatic Grouping for Mobile Devices on page 3-27* for details.
Automatic Grouping for Applications	Mobile Security adds Malware, Vulnerability and Privacy prefixes to group the mobile applications based on their risk levels. See *Automatic Status Update for Mobile Applications on page 3-28* for details.
Automatic Deployment of Mobile Security Client App	You can configure Citrix XenMobile to automatically deploy mobile device agent to mobile devices. • **Android**: See *Deploying Android Agent Through Mobile Security Server on page 3-31* for the procedure. • **iOS**: See *Deploying iOS Agent on page 3-32* for the procedure.

Automatic Grouping for Mobile Devices

Mobile Security uses prefixes to create three (3) classes (Dangerous, At Risk, Never Scanned, and Protected), and tags the risk devices as follows:

- TMMS_Security_Dangerous
- TMMS_Security_At Risk
- TMMS_Security_Never_Scanned
- TMMS_Security_Protected

For example, if Mobile Security detects a malware on a mobile device, it automatically changes the mobile device status as TMMS_Security_Dangerous.

Automatic Status Update for Mobile Applications

Mobile Security automatically adds a lable to the risky applications under App Groups, based on the type of risk they pose.

- TMMS_Security _Malware_App_Android
- TMMS_Security _Privacy_App_Android
- TMMS_Security _Vulnerability_App_Android
- TMMS_Security _Malware_App_iOS

Configuring Citrix XenMobile Integration

Procedure

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.
3. Click **Administration** > **Deployment Settings**.
4. Under **Server** section, select **Security Scan**, and then select **Citrix XenMobile** MDM Solution from the drop down list.
5. Under section **Service Registration**, configure Citrix XenMobile settings.
6. Click **Verify Settings** to make sure Mobile Security can connect to the Citrix XenMobile server.
7. Under **Data Synchronization Settings** section, select **Enable Data Synchronization** if you want to synchronize data, and then click **Synchronize Now**.

8. Under **Notification Setting** section, select **Automatically send invitation email to user** to send an email notification automatically to the user whenever a new user is synchronized from Citrix XenMobile server.

Agent Deployment

Trend Micro Mobile Security enables you to deploy client agent from the two different sources:

- **Google Play Store**: You will need to configure Citrix XenMobile to deploy the mobile device agent and provide the enrollment information to users, in the form of text or a QR-code. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen.

  After installing the mobile device agent, users will be required to enroll to the Mobile Security server manually. If you deploy mobile device agent from Google Play Store, the mobile device users can receive the real-time updates via Google Play.

- **Mobile Security Server**: Notify users to download the mobile device agent, with the name: **ENT Security**, from Citrix XenMobile app store.

  If you use this deployment option, you will need to provide the enrollment information to users, in the form of text or a QR-code. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen. Whenever a user launches the mobile device agent, the user will need to enroll the app to the Mobile Security server. You can also configure the app to enroll automatically. However, whenever there is an update available, the mobile device users will be required to update their mobile device agents manually.

Deploying Android Agent Through Google Play Store

Procedure

1. Log on to the Citrix XenMobile web console, and click **Configure** > **Apps**.
2. Click **Add**, and then click **Public App Store**.
3. In the **Name** field, type `ENT Security` .
4. Add the description for **Enterprise Mobile Security**, and from the **Category** drop-down list, select the category where you want to place this application, and then click **Next**.
5. Select **Google Play**, under **Platform** from the left menu, and clear all others.
6. Type `ENT Security` in the search filed, and click **Search**.
7. Click **Enterprise Mobile Security**, and modify the app details if required, and then click **Next**.
8. On **Approvals (optional)** screen, modify the settings if required, and then click **Next**.
9. On the **Delivery Group Assignments (optional)** screen, select the groups you want to assign and modify the settings if required.
10. Click **Save**.

What to do next

Provide the enrollment information to users, in the form of text or a QR-code after deploying the Android agent. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen.

Deploying Android Agent Through Mobile Security Server

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Administration** > **Device Enrollment Settings** on the menu bar.
3. On the **Authentication** tab, select **Authenticate using Enrollment Key**, and then select **Use preset Enrollment Key**.
4. Click **Administration** > **Deployment Settings** > **Android Agent (tab)**.
5. Select **Download from Trend Micro Mobile Security Server**.
6. If you want to enroll users automatically, select **Auto Enrollment**.
7. Click **Save** to save the settings.
8. Click **Upload**, and then select the modified Mobile Security agent file to upload it to the Citrix XenMobile server.

   The mobile device agent uploads and appears on the Citrix XenMobile administration web console.
9. Log on to the Citrix XenMobile web console, and click **Configure** > **Apps**.
10. Select **ENT Security** app from the application list, and then click **Edit**.
11. Click **Delivery Group Assignments (optional)** from the left menu, and select the groups you want to assign, and modify the settings if required.
12. Click **Save**.

What to do next

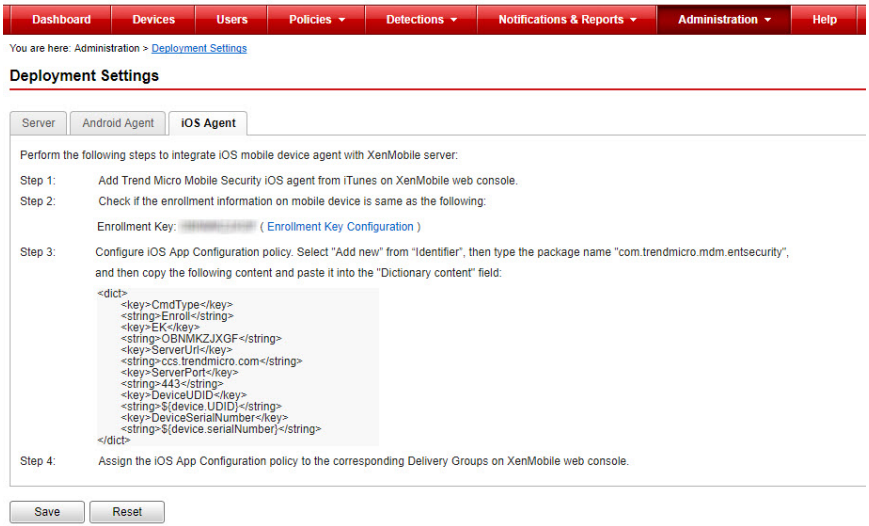
If you did not select the **Auto Enrollment** setting, provide the enrollment information to users, in the form of text or a QR-code after deploying the Android agent. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen.

Deploying iOS Agent

Procedure

1. Log on to the Citrix XenMobile web console, and click **Configure** > **Device Policies**.
2. Click **Add**.
3. Click **App Configuration** from the main screen.
4. Type the **Policy Name** and **Description** in the fileds provided, and then click **Next**.
5. Select **iOS** from the left menu, and clear all other platforms.
6. On the **App Configuration Policy** screen, select **Add new** from the **Identifier** drop-down list.
7. Type the identifier name and the enrollment key information in the **Dictionary content** field.

   For the **Identifier** name and **Dictionary content**, refer to **Mobile Security web console** > **Administration** > **Deployment Settings** > **iOS Agent (tab)**



8. Click **Check Disctionary** to verify dictionary content.
9. Click **Next**.
10. On the **App Configuration Policy** screen, select the groups you want to assign and modify the settings if required.
11. Click **Save**.
12. Click **Configure** > **Apps**.
13. Click **Add**, and then click **Public App Store**.
14. In the **Name** field, type `ENT Security`.
15. Add the description for **Enterprise Mobile Security**, and from the **Category** drop-down list, select the category where you want to place this application, and then click **Next**.
16. Select **iPhone** and/or **iPad**, under **Platform** from the left menu, and clear all others.
17. Type `ENT Security` in the search filed, and click **Search**.

18. Click **Enterprise Mobile Security**, and modify the app details if required, and then click **Next**.
19. On **Approvals (optional)** screen, modify the settings if required, and then click **Next**.
20. On the **Delivery Group Assignments (optional)** screen, select the groups you want to assign and modify the settings if required.
21. Click **Save**.

Integration with IBM MaaS360

Trend Micro Mobile Security enables you to integrate IBM MaaS360 MDM solution with Mobile Security.

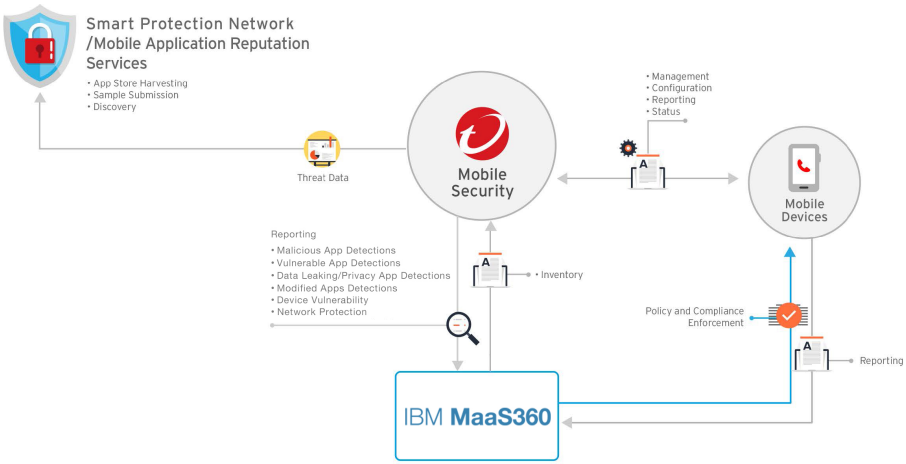
Prerequisites for Integration

To integrate other MDM solutions with Trend MicroMobile Security, you must use the following:

- Mobile Security for Enterprise 9.8 SP5 Critical Patch 3 or later
- Local Communication Server or Cloud Communication Server configured in Mobile Security

IBM MaaS360 Integration Architecture

The following image shows the high-level architecture of integration with IBM MaaS360.



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. It is the world's first automatic mobile app evaluation service.

The **Trend Micro Smart Protection Network** delivers proactive global threat intelligence against zero-hour threats to ensure that you are always protected. Trend Micro uses the up-to-the-second threat intelligence to immediately stamp out attacks before they can harm you. The **Smart Protection Network** is powering all of Trend Micro products and services.

Mobile Security uses Smart Protection Network and Mobile Application Reputation Services to find mobile device security issues and leverages IBM MaaS360 compliance policy to manage your mobile device.

Integration Features

Trend MicroMobile Security provides the following features with integration with IBM MaaS360:

Feature	Description
Automatic Grouping for Mobile Devices	Mobile Security adds Dangerous, Risky, No_TMMS suffixes to tag the mobile devises based on their risk levels. See *Automatic Grouping for Mobile Devices on page 3-27* for details.

Automatic Grouping for Mobile Devices

Mobile Security uses prefixes to create three (3) classes (Dangerous, Risky and NO_TMMS), and tags the risk devices as follows:

- PREDEFINEDPREFIX_Dangerous
- PREDEFINEDPREFIX _Risky
- PREDEFINEDPREFIX _NO_TMMS

Mobile Security enables you to define prefixes (PREDEFINEDPREFIX) on the administration web console. While Mobile Security detects a mobile device with different security levels, it automatically changes the device's Custom Attribute value.

For example, if Mobile Security detects that a malware on a mobile device, it automatically moves the mobile device to PREDEFINEDPREFIX _Dangerous group.

Configuring IBM MaaS360 Integration

Procedure

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.

3. Click **Administration** > **Deployment Settings**.
4. Under **Server** section, select **Security Scan**, and then select **IBM MaaS360** MDM Solution from the drop down list.
5. Under section **Service Registration**, configure IBM MaaS360 settings.
6. Click **Verify Settings** to make sure Mobile Security can connect to the IBM MaaS360 server.
7. Under **Data Synchronization Settings** section, select **Enable Data Synchronization** if you want to synchronize data, and then click **Synchronize Now**.
8. Under **Notification Setting** section, select **Automatically send invitation email to user** to send an email notification automatically to the user whenever a new user is synchronized from IBM MaaS360 server.

Agent Deployment

Trend Micro Mobile Security enables you to deploy client agent from the two different sources:

- **Google Play Store**: You will need to configure IBM MaaS360 to deploy the mobile device agent and provide the enrollment information to users, in the form of text or a QR-code. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen.

  After installing the mobile device agent, users will be required to enroll to the Mobile Security server manually. If you deploy mobile device agent from Google Play Store, the mobile device users can receive the real-time updates via Google Play.

- **Mobile Security Server**: Notify users to download the mobile device agent, with the name: **ENT Security**, from IBM MaaS360 app store.

  If you use this deployment option, you will need to provide the enrollment information to users, in the form of text or a QR-code. The

users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen. Whenever a user launches the mobile device agent, the user will need to enroll the app to the Mobile Security server. You can also configure the app to enroll automatically. However, whenever there is an update available, the mobile device users will be required to update their mobile device agents manually.

Deploying Android Agent Through Google Play Store

Procedure

1. Log on to IBM MaaS360 web console, and click **App** > **Catalog** on the menu bar.
2. Click **Add**, and then select **Android** > **Google Play App**.
3. Type `ENT Security` in the **App** field, and then click **Enterprise Mobile Security**, from the search results.
4. On the **App Catalog** screen, click **Distribute** under the **Enterprise Mobile Security** app name.
5. Select **All Devices**, **Group** or **Specific Devices** from the **Target** drop down list, and type the group or mobile device's name in the field provided, and then click **Distribute**.
6. If required, type your password on the pop-up screen.

   The application is distributed successfully to the selected mobile devices or groups.
7. After enrolling mobile device to MaaS360 server, start **App Catalog** app, and then tap the **Enterprise Mobile Security** app from the **Apps** list.
8. Tap **Install** to install the application to the mobile device.

Deploying Android Agent Through Mobile Security Server

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Administration** > **Device Enrollment Settings** on the menu bar.
3. On the **Authentication** tab, select **Authenticate using Enrollment Key**, and then select **Use preset Enrollment Key**.
4. Click **Administration** > **Deployment Settings** > **Android Agent (tab)**.
5. Select **Download from TMMS Server**, and then select **Auto Enrollment**.
6. Click **Save** to save the settings.
7. Click **Upload** to upload it to the IBM MaaS360 server.

   The mobile device agent uploads and appears on the IBM MaaS360 administration web console.
8. On the **App Catalog** screen, click **Distribute** under the **Enterprise Mobile Security** app name.
9. Select **All Devices**, **Group** or **Specific Devices** from the **Target** drop down list, and type the group or mobile device's name in the field provided, and then click **Distribute**.
10. If required, type your password on the pop-up screen.

    The application is distributed successfully to the selected mobile devices or groups.
11. After enrolling mobile device to MaaS360 server, start **App Catalog** app, and then tap the **Enterprise Mobile Security** app from the **Apps** list.
12. Tap **Install** to install the application to the mobile device.

What to do next

If you did not select the **Auto Enrollment** setting, provide the enrollment information to users, in the form of text or a QR-code after deploying the

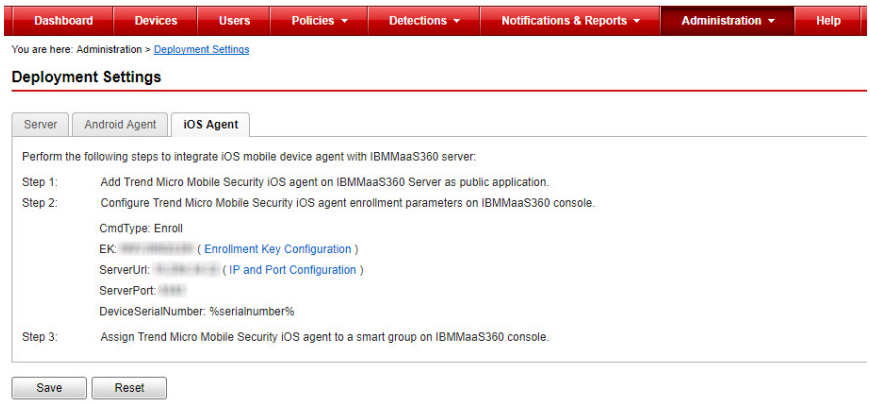
Android agent. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen.

Deploying iOS Agent

Procedure

1. Log on to IBM MaaS360 web console, and click **App** > **Catalog** on the menu bar.
2. Click **Add**, and then select **iOS** > **iTunes App Store App**.
3. Type `ENT Security` in the **App** field, and then click **Enterprise Mobile Security**, from the search results.
4. Without changing the information, click **Configuration**.
5. From the **App Config Source** drop-down list, select **Key/Value**.
6. Configure the enrollment parameters in the fields provided.

   For the enrollment parameters, refer to **Mobile Security web console** > **Administration** > **Deployment Settings** > **iOS Agent (tab)**



7. Click **Add**.

8. If required, type your password on the pop-up screen.

   The application adds successfully to the IBM MaaS360 server, and the **Enterprise Mobile Security** application is now displayed on the **App Catalog** screen.

9. On the **App Catalog** screen, click **Distribute** under the **Enterprise Mobile Security** app name.

10. Select **All Devices**, **Group** or **Specific Devices** from the **Target** drop down list, and type the group or mobile device's name in the field provided, and then click **Distribute**.

11. If required, type your password on the pop-up screen.

    The application is distributed successfully to the selected mobile devices or groups.

12. After enrolling mobile device to MaaS360 server, start **App Catalog** app, and then tap the **Enterprise Mobile Security** app from the **Apps** list.

13. Tap **Install** to install the application to the mobile device.

Integration with BlackBerry UEM

Trend Micro Mobile Security enables you to integrate BlackBerry UEM MDM solution with Mobile Security.

Note

Currently, Trend Micro Mobile Security supports integration with only on-premise BlackBerry UEM MDM solution.

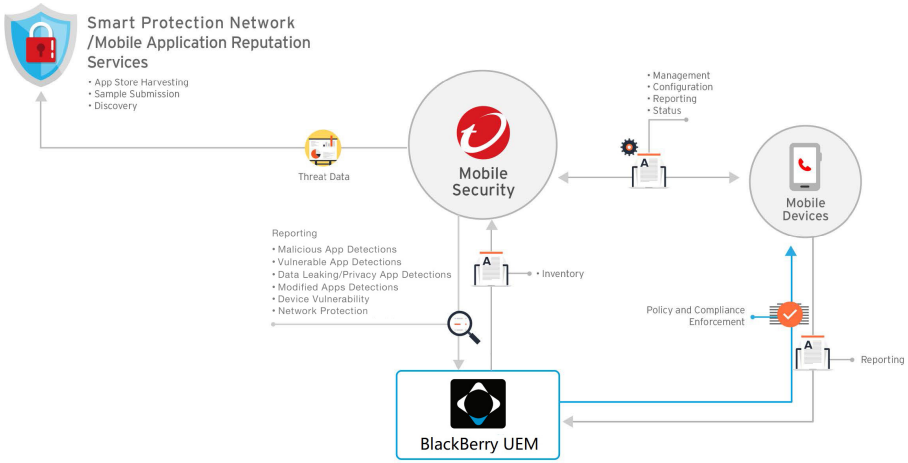
Prerequisites for Integration

To integrate other MDM solutions with Trend Micro Mobile Security, you must use the following:

- Mobile Security for Enterprise 9.8 SP5 Critical Patch 3 or later
- Local Communication Server or Cloud Communication Server configured in Mobile Security

BlackBerry UEM Integration Architecture

The following image shows the high-level architecture of integration with BlackBerry UEM.



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. It is the world's first automatic mobile app evaluation service.

The **Trend Micro Smart Protection Network** delivers proactive global threat intelligence against zero-hour threats to ensure that you are always protected. Trend Micro uses the up-to-the-second threat intelligence to immediately stamp out attacks before they can harm you. The **Smart Protection Network** is powering all of Trend Micro products and services.

Mobile Security uses Smart Protection Network and Mobile Application Reputation Services to find mobile device security issues and leverages BlackBerry UEM compliance policy to manage your mobile device.

Integration Features

Trend MicroMobile Security provides the following features with integration with BlackBerry UEM:

Feature	Description
Automatic Deployment of Mobile Security Client App	You can configure BlackBerry UEM to automatically deploy mobile device agent to mobile devices. • **Android**: See *Deploying Android Agent Through Mobile Security Server on page 3-46* for the procedure. • **iOS**: See *Deploying iOS Agent on page 3-46* for the procedure.

Configuring BlackBerry UEM Integration

Procedure

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.

3. Click **Administration** > **Deployment Settings**.
4. Under **Server** section, select **Security Scan**, and then select **BlackBerry UEM On-Premise** MDM Solution from the drop down list.
5. Under section **Service Registration**, configure BlackBerry UEM settings.
6. Click **Verify Settings** to make sure Mobile Security can connect to the BlackBerry UEM server.
7. Under **Data Synchronization Settings** section, select **Enable Data Synchronization** if you want to synchronize data, and then click **Synchronize Now**.
8. Under **Notification Setting** section, select **Automatically send invitation email to user** to send an email notification automatically to the user whenever a new user is synchronized from BlackBerry UEM server.

Agent Deployment

Trend Micro Mobile Security enables you to deploy client agent from the two different sources:

- **Google Play Store**: You will need to configure BlackBerry UEM to deploy the mobile device agent and provide the enrollment information to users, in the form of text or a QR-code. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen.

  After installing the mobile device agent, users will be required to enroll to the Mobile Security server manually. If you deploy mobile device agent from Google Play Store, the mobile device users can receive the real-time updates via Google Play.

- **Mobile Security Server**: Notify users to download the mobile device agent, with the name: **ENT Security**, from BlackBerry UEM app store.

  If you use this deployment option, you will need to provide the enrollment information to users, in the form of text or a QR-code. The

users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen. Whenever a user launches the mobile device agent, the user will need to enroll the app to the Mobile Security server. You can also configure the app to enroll automatically. However, whenever there is an update available, the mobile device users will be required to update their mobile device agents manually.

Deploying Android Agent Through Google Play Store

Procedure

1. Log on to BlackBerry UEM web console, and click **Apps** > **Apps**.
2. Click the add icon, and then click **Google Play**.
3. In the **Name** field, type `Enterprise Mobile Security`.
4. Click **Approve**.
5. Enable **Keep approved when app requests new permissions** and click **Done**.
6. Keep the default settings and click **Add**.

What to do next

Provide the enrollment information to users, in the form of text or a QR-code after deploying the Android agent. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen.

Deploying Android Agent Through Mobile Security Server

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Administration** > **Device Enrollment Settings** on the menu bar.
3. On the **Authentication** tab, select **Authenticate using Enrollment Key**, and then select **Use preset Enrollment Key**.
4. Click **Administration** > **Deployment Settings** > **Android Agent (tab)**.
5. Select **Download from Trend Micro Mobile Security Server**.
6. If you want to enroll users automatically, select **Auto Enrollment**.
7. Click **Save** to save the settings.
8. Click **Upload**. The Android agent will be shown on **Apps** > **Apps** on the BlackBerry UEM web console.

What to do next

If you did not select the **Auto Enrollment** setting, provide the enrollment information to users, in the form of text or a QR-code after deploying the Android agent. The users can use the enrollment information or scan the QR code to enroll with the server. The enrollment information includes the server IP address and port number, and an enrollment key, which is available on the **Android Agent** tab on **Deployment Settings** screen.

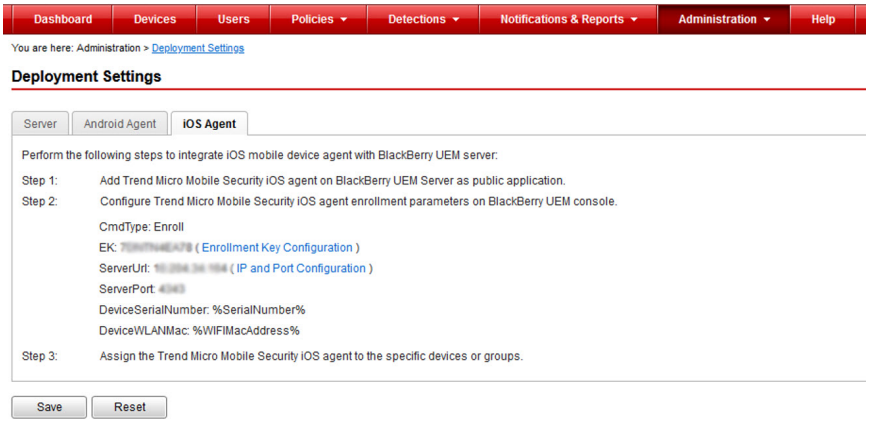
Deploying iOS Agent

Procedure

1. Log on to BlackBerry UEM web console, and click **Apps**.
2. Click the add icon, and then click **App Store**.
3. In the **Name** field, type `Enterprise Mobile Security`.

4. Click **Add** in the line of **Enterprise Mobile Security**.
5. In the **App Configuration** area, click the add icon to add application configuration.
6. Click **Configure manually**.
7. Type **App configuration name**, and set `Key` and `Value` to add configuration.

   For `Key` and `Value`, refer to **Mobile Security web console** > **Administration** > **Deployment Settings** > **iOS Agent (tab)**.



Configuration Key	Value Type	Configuration Value
CmdType	String	Enroll
EK	String	<Enrollment Key>
ServerUrl	String	<Actual server URL>
ServerPort	String	<Actual server port number>
DeviceSerialNumber	String	%SerialNumber%
DeviceWLANMac	String	%WIFIMacAddress%

8. Click **Save**.

9. Click **Add**.

Chapter 4

Managing Mobile Devices

This chapter helps you start using Mobile Security. It provides basic setup and usage instructions. Before you proceed, be sure to install the Management Server, Communication Server, and the Mobile Device Agent on mobile devices.

The chapter includes the following sections:

- *Managed Devices Tab on page 4-2*
- *Managing Groups on page 4-2*
- *Managing Mobile Devices on page 4-4*
- *Mobile Device Status on page 4-7*
- *Mobile Device Agent Tasks on page 4-9*
- *Updating Mobile Device Agents on page 4-10*
- *Integration with Trend Micro Control Manager on page 4-12*

Managed Devices Tab

The **Managed Devices** tab on the **Devices** screen enables you to perform tasks related to the settings, organization or searching of Mobile Device Agents. The toolbar above the device tree viewer lets you perform the following tasks:

- configure the device tree (such as creating, deleting, or renaming groups and creating or deleting Mobile Device Agents)
- configure Mobile Device Agents information
- search for and display Mobile Device Agent status
- on-demand Mobile Device Agent component update, scan device, and update policy
- export data for further analysis or backup

Groups in Mobile Security

Mobile Security Management Server automatically creates a root group **Mobile Devices** with the following sub-group:

- **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.

For instructions, refer to the Mobile Security Management Server *Online Help*.

Managing Groups

You can add, edit or delete groups under the **Mobile Devices** root group. However, you cannot rename or delete the root group **Mobile Devices** and the group **default**.

Adding a Group

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Devices** on the menu bar.

   The **Devices** screen displays.
3. On the **Managed Devices** tab, click the root group **Mobile Devices**, and then click **Add Group**.
4. Configure the following:
   - **Parent group**: Select the group under which you want to create a sub-group.
   - **Group name**: Type a name for the group.
   - **Policy**: Select the policy from the drop down list that you want to apply to the group.
5. Click **Add**.

Renaming a Group

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Devices** on the menu bar.

   The **Devices** screen displays.
3. On the **Managed Devices** tab, click the group that you want to rename.
4. Click **Edit**.
5. Modify the group name, and then click **Rename**.

Deleting a Group

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Devices** on the menu bar.

   The **Devices** screen displays.
3. On the **Managed Devices** tab, click the group that you want to delete.
4. Click **Delete**, and then click **OK** on the confirmation dialog box.

Managing Mobile Devices

You can edit mobile device information, delete mobile devices, or change the mobile device group on the **Devices** screen.

Reassigning Devices

Procedure

1. On to the Mobile Security administration web console, go to **Devices** > **Managed Devices**.

   The **Devices** screen displays.
2. From the device tree, select the device that you want to reassign.

   The device information appears.
3. Click **Change User**, and then modify the user name in the field provided.
4. Click **Save**.

Editing Mobile Device Information

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Devices** on the menu bar.

   The **Devices** screen displays.
3. On the **Managed Devices** tab, click the mobile device from the device tree whose information you want to edit.
4. Click **Edit**.
5. Update the information in the following fields:
   - **Phone Number**—the phone number of the mobile device. To ensure that the mobile device can receive notification messages successfully from an SMS sender, you may type the country code (1-5 digits long).
   - **Device Name**—the name of the mobile device to identify the device in the device tree.
   - **Group**—the name of the group to which the mobile device belongs from the drop-down list.
   - **Asset Number**—type the asset number assigned to the mobile device.
   - **Description**—any additional information or notes related to the mobile device or the user.
6. Click **Save**.

Deleting Mobile Devices

Mobile Security provides the following two options for deleting mobile devices:

- *Deleting Single Mobile Device on page 4-6*
- *Deleting Multiple Mobile Devices on page 4-6*

Deleting Single Mobile Device

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Devices** on the menu bar.

   The **Devices** screen displays.
3. On the **Managed Devices** tab, click the mobile device from the device tree that you want to delete.
4. Click **Delete** and then click **OK** on the confirmation dialog box.

The mobile device is deleted from the mobile device tree, and is no longer enrolled with the Mobile Security Management Server.

Deleting Multiple Mobile Devices

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Devices** on the menu bar.

   The **Devices** screen displays.
3. On the **Managed Devices** tab, click the group from the device tree whose mobile devices you want to delete.
4. Select the mobile devices from the list on the right pane, click **Delete** and then click **OK** on the confirmation dialog box.

The mobile devices are deleted from the mobile device tree, and are no longer enrolled with the Mobile Security Management Server.

Moving Mobile Devices to Another Group

You can move mobile devices from one group to another. Mobile Security will automatically send the notification to the user about the policies that you have applied to the group.

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Devices** on the menu bar.

   The **Devices** screen displays.
3. On the **Managed Devices** tab, click the group whose mobile devices you want to move to another group.
4. Select the mobile devices from the list on the right pane and then click **Move**.

   The **Move Devices** dialog box displays.
5. From the drop-down list, select the target group and then click **OK**.

Mobile Device Status

On the **Managed Devices** tab in the **Devices** screen, select the mobile device to display its status information on the right-pane. Mobile device information is divided into the following sections:

- **Basic**—includes registration status, phone number, LDAP Account, and platform information.
- **Hardware, Operating System**—shows the detailed mobile device information including device and model names, operating system

version, memory information, cellular technology, IMEI and MEID numbers, and firmware version information.

- **Security**—displays the mobile device's statuses for jailbreak/root, developer options, USB debugging, network traffic decryption; number of malicious iOS profiles, malicious SSL certificates, malicious applications, modified applications, vulnerable applications, privacy leaking applications; and the connected access point (Wi-Fi).

Basic Mobile Device Agent Search

To search for a Mobile Device Agent based on the mobile device name or phone number, type the information in the search field available on the **Devices** screen and click **Search**. The search result displays in the device tree.

Advanced Mobile Device Agent Search

You can use the **Advanced search** screen to specify more Mobile Device Agent search criteria.

Procedure

1. In the **Devices** screen, click the **Advanced search** link. A pop-up window displays.
2. Select the search criteria and type the values in the fields provided (if applicable):
   - **Device Name**—descriptive name that identifies a mobile device
   - **Phone Number**—phone number of a mobile device
   - **User Name**—user name of a mobile device
   - **Asset Number**—asset number of a mobile device
   - **IMEI**—IMEI number of a mobile device

- **Serial Number**—serial number of a mobile device
- **Wi-Fi MAC Address**—Wi-Fi MAC address of a mobile device
- **Description**— description of a mobile device
- **Operating System**—confine the search to the specific operating system the mobile device is running; or to the version number for Android and iOS
- **Group**—group to which the mobile device belongs
- **Agent Version**—Mobile Device Agents version number on the mobile device
- **Last Connected**—time range in which a mobile device was last connected to the Mobile Security server
- **Malware Pattern Version**—Malware Pattern file version number on the mobile device
- **Malware Scan Engine Version**—Malware Scan Engine version number of the mobile device
- **App Name**—application installed on mobile devices
- **Infected mobile device agent**—confine the search to mobile devices with the specified number of detected malware

3. Click **Search**. The search result displays in the device tree.

Mobile Device Agent Tasks

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

Updating Mobile Device Agents

You can send the update notification to mobile devices with out-of-date components or security policies from the **Managed Devices** tab in **Devices** screen.

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Devices** on the menu bar.

   The **Devices** screen displays.
3. On the **Managed Devices** tab, click the group whose mobile devices you want to update.
4. Click **Update**.

Mobile Security sends the update notification to all the mobile devices with out-of-date components or security policies.

You can also use the **Update** screen to set Mobile Security to automatically send update notification to mobile devices with out-of-date components or policies or initiate the process manually.

See *Updating Mobile Security Components on page 8-2* for more information.

Updating Mobile Device Information

The Mobile Security server automatically obtains the device information from managed mobile devices at scheduled intervals and displays the device information on the **Devices** screen.

You can update the device information of a managed device on the **Managed Devices** tab before the next scheduled automatic update.

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Devices** on the menu bar.

   The **Devices** screen displays.
3. On the **Managed Devices** tab, select a mobile device from the device tree.
4. Click **Update**.

Exporting Data

You can export data for further analysis or a backup from the **Managed Devices** tab on **Devices** screen.

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Devices** on the menu bar.

   The **Devices** screen displays.
3. Select the mobile device group from the device tree whose data you want to export.
4. Click **Export**.
5. If required, click **Save** on the pop-up that appears to save the `.zip` file on your computer.
6. Extract the downloaded `.zip` file content and open the `.csv` file to view the mobile device information.

Integration with Trend Micro Control Manager

Trend Micro Mobile Security provides integration with Trend Micro Control Manager (also referred to as Control Manager or TMCM). This integration enables the Control Manager administrator to:

- create, edit or delete security policies for Mobile Security
- deliver security policies to enrolled mobile devices
- view Mobile Security **Dashboard** screen

For the detailed information about Trend Micro Control Manager and handling Mobile Security policies on Control Manager, refer to the product documentation at the following URL:

http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx

Creating Security Policies in Control Manager

The Trend Micro Control Manager web console displays the same security policies that are available in Mobile Security. If a Control Manager administrator creates a security policy for Mobile Security, Mobile Security will create a new group for this policy and move all the target mobile devices to this group. To differentiate the policies that are created in Mobile Security with the policies created in Control Manager, Mobile Security adds a prefix **TMCM_** to the group name.

Deleting or Modifying Security Policies

The Control Manager administrator can modify a policy at any time and the policy will be deployed to the mobile devices immediately.

Trend Micro Control Manager synchronizes the policies with Trend Micro Mobile Security after every 24 hours. If you delete or modify a policy that is created and deployed from Control Manager, the policy will be reverted to the original settings or created again after the synchronization occurs.

Security Policy Statuses on Control Manager

On the Trend Micro Control Manager web console, the following statuses are displayed for the security policies:

- **Pending**: The policy is created on the Control Manager web console and has not yet been delivered to the mobile devices.
- **Deployed**: The policy has been delivered and deployed on all the target mobile devices.

Chapter 5

Viewing Users

This chapter shows you how to view users that are registered with Mobile Security.

The chapter includes the following sections:

- *Users Tab on page 5-2*
- *Viewing the Users List on page 5-2*

Users Tab

You can use the **Users** tab to view all the mobile devices that are registered with Mobile Security.

Viewing the Users List

Procedure

1. On the Mobile Security administration web console, go to **Users**.

   The **Users** screen appears.

2. To sort the list, click the header for any of the following columns.

   - User Name
   - Email
   - Devices
   - Invited On

3. To search for a user, type the user name or email address in the **Search** bar and then press Enter.

   If the user is in the list, Mobile Security displays the information.

Chapter 6

Protecting Devices with Policies

This chapter shows you how to configure and apply security policies to mobile devices in a Mobile Security group. You can use policies related to provisioning, device security and data protection.

The chapter includes the following sections:

- *About Policies on page 6-2*
- *Policies for All Devices on page 6-2*
- *Managing Policies for All Devices on page 6-3*
- *Policies for All Groups on page 6-6*
- *Managing Policies for All Groups on page 6-10*

About Policies

You can configure policies for a Mobile Security group on the Management Server or all the mobile devices that are enrolled with Mobile Security.

TABLE 6-1. Device Policies in Mobile Security

POLICY	REFERENCE
Approved List	See *Application Approved List on page 6-2*.
Trusted Network Traffic Decryption Certificate List	See *Trusted Network Traffic Decryption Certificate List on page 6-3*.

TABLE 6-2. Group Policies in Mobile Security

POLICY GROUP	POLICY	REFERENCE
General	Common Policy	See *Common Policy on page 6-6*.
Device Security	Security Policy	See *Security Policy on page 6-7*.

Policies for All Devices

This section introduces the policies that are available in Mobile Security for all mobile devices.

Application Approved List

The **Application Approved List** includes all the applications that are detected as security risk (malware, vulnerable, privacy risk or modified), but are approved by the administrator for installation on mobile devices.

To manage **Application Approved List**, click **Policies** > **Policies For All Devices**.

Trusted Network Traffic Decryption Certificate List

If there is an SSL certificate that Mobile Security detects as malicious, it will display these certificates on **Detections** > **Malicious SSL Certificates** screen. However, you can add those "malicious" certificates to the **Trusted Network Traffic Decryption Certificate List** to enable Mobile Security to skip these certificates during scanning, and hide them from the **Malicious SSL Certificates** screen.

To manage **Trusted Network Traffic Decryption Certificate List**, click **Policies** > **Policies For All Devices**.

Managing Policies for All Devices

Mobile Security enables you to maintain an application approved list and a trusted network traffic decryption certificate list to allow users to use these applications and network decryption certificates without restrictions or warnings.

Use the **Policy For All Devices** screen to create, edit, copy or delete policies for mobile devices.

Adding Applications to Approved List

Procedure

1. Log on to the Mobile Security administration web console.
2. Do one of the following:
   - Add an application already installed and scanned by Mobile Security to the **Approved List**.
     a. Click **Detections** > **Application Security Status** on the menu bar.
     b. Click **Android** or **iOS** tab, and select the applications from the list of detected applications that you want to add to the **Approved List**.

c. Click **Add to Approved List**.

- Add applications manually to the **Approved List**.

  a. Click **Policies** > **Policies For All Devices** on the menu bar.

  b. Under **Applications Approved List** section, click **Android** or **iOS** tab, and then click **Add to Approved List**.

     The **Import Application** screen appears.

  c. Type the application ID, name and description in the filed provided. Use semicolon (;) to separate each application information.

  d. Click **Save** on **Import Application** screen.

  e. Click **Save** on **Policy For All Devices** screen.

Removing Applications from Approved List

Procedure

1. Log on to the Mobile Security administration web console.
2. Do one of the following:

   - Remove applications that are already installed and scanned by Mobile Security from the **Approved List**.

     a. Click **Detections** > **Application Security Status** on the menu bar.

     b. Click **Android** or **iOS** tab, and select the applications from the list of detected applications that you want to remove from the **Approved List**.

     c. Click **Remove from Approved List**.

   - Remove an application directly from to the **Approved List**.

a. Click **Policies** > **Policies For All Devices** on the menu bar.

b. Under **Applications Approved List** section, click **Android** or **iOS** tab, and then select applications that you want to remove from the list.

c. Click **Remove from Approved List**.

d. Click **Save** on **Policy For All Devices** screen.

Adding a Trusted Network Traffic Decryption Certificate

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Policies** > **Policies For All Devices** on the menu bar.

   The **Policy For All Devices** screen appears.
3. Under **Trusted Network Traffic Decryption Certificate List** section, click **Add**.

   The **Add Certificate** screen appears.
4. Select a certificate file from your local hard drive, and type a description for the certificate file in **Description** field.
5. Click **OK**.
6. Click **Save** on **Policy For All Devices** screen.

Deleting a Trusted Network Traffic Decryption Certificate

Procedure

1. Log on to the Mobile Security administration web console.

2. Click **Policies** > **Policies For All Devices** on the menu bar.

   The **Policy For All Devices** screen appears.

3. Under **Trusted Network Traffic Decryption Certificate List** section, select the certificate files that you want to delete, and then click **Delete**.

4. Click **Save** on **Policy For All Devices** screen.

Policies for All Groups

This section introduces the policies that are available in Mobile Security for all groups.

Using the superuser account, you can specify any policy as a template for group admins to create further security policies in Mobile Security. However, once you specify a security policy as a template, you cannot assign that security policy to any group.

Common Policy

Common Policy provides the common security policies for mobile devices. To configure common security policy settings, click **Policies**, then click the policy name, and then click **Common Policy**.

- **User Privileges**:
  - You can select whether to allow users to configure Mobile Security device agent settings.

    If you do not select the **Allow users to configure Mobile Security client settings** check box, users cannot change Mobile Device Agent settings. However, the filtering lists for **Web Threat Protection Policy** are not affected when this option is selected. For more information, see *Security Policy on page 6-7*.

- You can select the auto-check option to have Mobile Device Agents periodically check for any component or configuration updates on the Mobile Security Management Server.

Security Policy

You can configure the **Security Settings** from the **Security Policy** screen.

Note

Mobile Security Web Threat Protection only supports the default Android browser and Google Chrome on mobile devices.

To configure the security protection policy settings, click **Policies**, click the policy name, and then click **Security Policy**.

The following table describes the available settings for this policy.

TABLE 6-3. Security Policy Settings

SECTION	ITEM	DESCRIPTION	SUPPORTED MOBILE DEVICE OS
Security Setting	**Scan installed applications only**	Select this option if you want to scan installed applications only	
	Scan installed applications and files	Select this option if you want to scan installed applications and other files stored on the mobile device. If you select this option, specify whether you want to scan only APK files or all files.	
	Scan after pattern update	Enable this option if you want to run the malware scan after every pattern update. Mobile Security runs a scan automatically after successful	

Section	Item	Description	Supported Mobile Device OS
		pattern update on Android mobile devices.	
	Application scan	Enable this option if you want to scan applications for malware, privacy risks, vulnerable and modified (repackaged) applications.	
	Network security scan	These settings scan for network traffic decryption, unsafe access points (Wi-Fi) or installed malicious SSL certificates. All options under this category are enabled by default and cannot be modified.	
	Vulnerable applications scan	These settings scan the mobile device for vulnerability due to USB debugging, developer options, malicious profiles, and rooted or jailbroken mobile devices.	
	Block network when Network Traffic Decryption is detected	Enable this option to stop the network traffic decryption when Mobile Security detects the leakage of data during communication.	
	Block network when suspicious access point (Wi-Fi) is detected as high risk	Enable this option to disconnect mobile devices from the network, when the network connection is detected as suspicious of being fake.	
	Enable scheduled scan under **Scan Schedule**	Select **Daily**, **Weekly** or **Monthly** to run the scan every day, once a week, or once a month, respectively.	

Section	Item	Description	Supported Mobile Device OS
Web Threat Protection Setting	**Enable central controlled Web Threat Protection policy**	This feature provides you server-side control of web threat protection policies. You can configure the following protection levels according to your requirements: • **Low**: This setting provides the least protection against online fraud and other malicious activities from Web sites. • **Normal**: This setting provides protection against online security threats, without blocking most Web sites. Trend Micro recommends this default setting. • **High**: This setting provides the most protection against online fraud and other Web sites; allows opening Web sites with a very good reputation, and blocks all others.	
	Filter Lists	Mobile Security will block all the URLs that you add in the **Blocked List**, and allow all the URLs that are in the **Approved List**.	
	Reassess URL	If you come across a URL that you think has been misclassified, you can notify Trend Micro of any such URL through the following website: http://sitesafety.trendmicro.com/	

Managing Policies for All Groups

Mobile Security enables you to quickly create a policy using the default policy templates.

Use the **Policy For All Groups** screen to create, edit, copy or delete policies for mobile devices.

Creating a Policy

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Policies** > **Policies For Groups** on the menu bar.

   The **Policy** screen displays.
3. Click **Create**.

   The **Create Policy** screen displays.
4. Type the policy name and description in their respective fields and then click **Save**.

   Mobile Security creates a policy with the default settings. However, the policy is not assigned to a group. To assign the policy to a group, see *Assigning or Removing Policy from a Group on page 6-11*.
5. (Super Administrator only) If you want to use this policy as a template, click the arrow button under the **Type** column on the **Policy** screen. The group administrators can use templates created by the Super Administrator to create policies for their assigned groups.

Note

- You cannot assign a template to any group.
- You can also convert a template to policy. However, you can only convert a template to policy if the template is not assigned to any group.

Editing a Policy

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Policies** > **Policies For Groups** on the menu bar.

   The **Policy** screen displays.
3. In the policy list, click the policy name whose details you want to edit.

   The **Edit Policy** screen displays.
4. Modify the policy details and then click **Save**.

Assigning or Removing Policy from a Group

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Policies** > **Policies For Groups** on the menu bar.

   The **Policy** screen displays.
3. In the **Applied Groups** column of a policy, click the group name. If the policy is not assigned to a group, click **None**.
4. Do one of the following:

- To assign a policy to a group: from the **Available groups** list on the left side, select the group to which you want to apply the policy, and then click **>** to move the group to the right side.
- To remove policy from a group: from the group list on the right side, select a group that you want to remove, and then click **<** to move the group to the **Available groups** list on the left side.

5. Click **Save**.

Copying a Policy

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Policies** > **Policies For Groups** on the menu bar.

   The **Policy** screen displays.
3. Select the policy that you want to copy, and then click **Copy**.

Deleting Policies

You cannot delete the **Default** policy and any policy that is applied to a group. Make sure to remove the policy from all the groups before deleting a policy. See *Assigning or Removing Policy from a Group on page 6-11* for the procedure.

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Policies** > **Policies For Groups** on the menu bar.

   The **Policy** screen displays.
3. Select the policy that you want to delete, and then click **Delete**.

Chapter 7

Viewing and Managing Detections

This chapter shows you how to manage detected malicious applications for iOS and Android mobile devices, and viewing SSL certificates and iOS profiles.

The chapter includes the following sections:

- *About Suspicious Applications Screen on page 7-2*
- *Viewing Malicious SSL Certificates on page 7-6*
- *Viewing Malicious iOS Profiles on page 7-7*

About Suspicious Applications Screen

The **Suspicious Applications** screen displays the application name, version, security scan status, number of installations and the last time of scan for all the applications that are installed on mobile devices.

You can also add the applications that are displayed on this screen, to the **Approved List** of applications, if you consider any of these applications as safe. Similarly, you can also remove the applications that you have previously added to the **Approved List**, but now you do not consider them as safe.

Refer to *Adding Applications to Approved List on page 6-3* and *Removing Applications from Approved List on page 6-4* for the procedures.

Click on **Manage Approved List** link at the top-right of the table to navigate to the **Approved List** screen to manage the list.

The following table lists the information available for Android and iOS apps.

TABLE 7-1. Application Security Statuses

INFORMATION	DESCRIPTION	ANDROID	IOS
App name	Name of the app	●	●
Version	App version number	●	●

Information	Description	Android	iOS
Malware scan result	The malware scan may have any of the following results: • **Normal**—No malware detected • **PUA**—Potentially unwanted applications or PUAs are grayware apps that could possibly pose a high risk on user security and/or privacy. For more information, see http://www.trendmicro.com/vinfo/us/security/definition/potentially-unwanted-app. • **Malware**—Known malware • **Unknown**—No information available	●	●
Vulnerability scan result	The vulnerability scan may have any of the following risk ratings: • **Normal** • **Medium** • **High** • **Unknown**—No information available	●	
Privacy scan result	The privacy scan may have any of the following risk ratings: • **Normal** • **Medium** • **High** • **Unknown**—No information available	●	

Information	Description	Android	iOS
Modified	The modified app scan may have any of the following results: • **Yes**—Original app was modified or repackaged for possibly malicious purposes • **No**—No modifications have been made to the original app • **Unknown**—No information available	●	●
Number of installations	Number of devices installed with the app	●	●
Last scanned	Date and time of the last scan	●	●

When Mobile Security scans applications for security risks, it takes the following actions based on the security scan results:

- Display the detection on the **Dashboard** screen on the **Android/iOS Application Risk Summary** widget
- Display the number of detected security risks for the mobile device on the **Devices** screen under relevant category
- Generate a log entry

Viewing Suspicious Android Applications

Procedure

1. On the Mobile Security web console, go to **Detections** > **Suspicious Applications** > **Android** tab.

   The **Android** tab appears.

2. To view the scan details of an app, click the result under any of the following columns.

- Vulnerability Scan Result
- Privacy Scan Result

The scan details page of the selected result appears.

3. To view the devices installed with an app, click the number under the **Number of Installations** column.

   The **Devices** screen appears and displays the list of devices under the **Managed Devices** tab.

4. To view information on a specific app, type the app name in the **Search** bar and then press Enter.

   If the app is in the list, the table displays the app information.

Viewing Suspicious iOS Applications

Procedure

1. On the Mobile Security web console, go to **Detections** > **Suspicious Applications** > **iOS** tab.

   The **iOS** tab appears.

2. To view the devices installed with an app, click the number under the **Number of Installations** column.

   The **Devices** screen appears and displays the list of devices under the **Managed Devices** tab.

3. To view information on a specific app, type the app name in the **Search** bar and then press Enter.

   If the app is in the list, the table displays the app information.

Viewing Malicious SSL Certificates

The **Malicious SSL Certificates** screen displays the SSL certificates that are detected as malicious by Mobile Security, and are installed on Android or iOS mobile devices. If you trust any of the certificates that are listed on **Malicious SSL Certificates** screen, you can add that certificate to the *Trusted Network Traffic Decryption Certificate List on page 6-3* to hide it from the **Malicious SSL Certificates** screen.

When Mobile Security detects a malicious certificate, it takes the following actions:

- Display the malicious SSL certificate on the **Malicious SSL Certificates** screen
- Display the detection on the **Dashboard** screen on the **Network Protection Summary** widget
- Update the device security status to **Dangerous**
- Send a notification email to the administrator
- Generate a log entry

The certificate details displayed on **Malicious SSL Certificates** screen include certificate name and details, number of installations on mobile devices and the last time of scan.

Procedure

1. On the Mobile Security web console, go to **Detections** > **Malicious SSL Certificates**.

   The **Malicious SSL Certificates** screen appears.

2. Click **Android** or **iOS** tab.

3. To view information on a specific app, type the app name in the **Search** bar and then press Enter.

If the app is in the list, the table displays the app information.

Viewing Malicious iOS Profiles

The **Malicious iOS Profiles** screen displays the iOS profiles that are detected as malicious by Mobile Security, and are installed on iOS mobile devices.

When Mobile Security detects a malicious iOS profile, it takes the following actions:

- Display the malicious iOS profile on the **Malicious iOS Profiles** screen
- Display the detection on the **Dashboard** screen on the **iOS Network Protection Summary** widget
- Update the device status to **Dangerous**
- Send a notification email to the administrator
- Generate a log entry

The profile details displayed on the **Malicious iOS Profiles** screen include profile name, its type, scan result, number of installations on mobile devices and the last time of scan.

Procedure

1. On the Mobile Security web console, go to **Detections** > **Malicious iOS Profiles**.

   The **Malicious iOS Profiles** screen appears.

2. To view information on a specific iOS profile, type the certificate name in the**Search** bar and then press **Enter**.

   If the certificate is in the list, the table displays the app information.

Chapter 8

Updating Components

This chapter shows you how to update Mobile Security components.

The chapter includes the following sections:

- *About Component Updates on page 8-2*
- *Updating Mobile Security Components on page 8-2*
- *Manually Updating a local AU server on page 8-5*

About Component Updates

In Mobile Security, the following components or files are updated through ActiveUpdate, the Trend Micro Internet-based component update feature:

- Mobile Security Server—program installation package for Mobile Security Communication Server.
- Malware Pattern—file containing thousands of malware signatures, and determines the ability of Mobile Security to detect hazardous files. Trend Micro updates pattern files regularly to ensure protection against the latest threats.
- Mobile Device Agents installation program—program installation package for the Mobile Device Agents.

Updating Mobile Security Components

You can configure scheduled or manual component updates on the Mobile Security Management Server to obtain the latest component files from the ActiveUpdate server. After a newer version of a component is downloaded on the Management Server, the Management Server automatically notifies mobile devices to update components.

Manual Update

You can perform a manual server and Mobile Device Agent update in the Manual tab on Updates screen. You should have already configured the download source in the Source screen (see *Specifying a Download Source on page 8-4* for more information).

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Administration** > **Updates**.

The **Updates** screen displays.

3. Click the **Manual** tab.
4. Select the check box of the component you want to update. Select the **Anti-Malware Components**, **Agent Installation Packages** and/or **Server Version** check box(es) to select all components in that group. This screen also displays the current version of each component and the time the component was last updated.

   See *About Component Updates on page 8-2* for more information on each update component.
5. Click **Update** to start the component update process.

Scheduled Update

Scheduled updates allow you to perform regular updates without user interaction; thereby, reducing your workload. You should have already configured the download source in the **Source** screen (refer to *Specifying a Download Source on page 8-4* for more information).

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Administration** > **Updates**.

   The **Updates** screen displays.
3. Click the **Scheduled** tab.
4. Select the check box of the component you want to update. Select the **Anti-Malware Components**, **Agent Installation Packages** and/or **Server Version** check box(es) to select all components in that group. This screen also displays each component's current version and the time the component was last updated.
5. Under **Update Schedule**, configure the time interval to perform a server update. The options are **Hourly**, **Daily**, **Weekly**, and **Monthly**.

- For weekly updates, specify the day of the week (for example, Sunday, Monday, and so on.)
- For monthly updates, specify the day of the month (for example, the first day, or 01, of the month and so on).

Note

The **Update for a period of x hours** feature is available for the `Daily`, `Weekly`, and `Monthly` options. This means that your update will take place sometime within the number of hours specified, following the time selected in the **Start time** field. This feature helps with load balancing on the ActiveUpdate server.

- Select the **Start time** when you want Mobile Security to initiate the update process.

6. Click **Save** to save the settings.

Specifying a Download Source

You can set Mobile Security to use the default ActiveUpdate source or a specified download source for server update.

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Administration** > **Updates**.

   The **Updates** screen displays. For more information about the update see *Manual Update on page 8-2* or for scheduled update see *Scheduled Update on page 8-3*.
3. Click the **Source** tab.
4. Select one of the following download sources:
   - **Trend Micro ActiveUpdate server**—the default update source.

- **Other update source**—specify HTTP or HTTPS website (for example, your local Intranet website), including the port number that should be used from where Mobile Device Agents can download updates.

  Note

  The updated components have to be available on the update source (web server). Provide the host name or IP address, and directory (for example, `https://12.1.123.123:14943/source`).

- **Intranet location containing a copy of the current file**—the local intranet update source. Specify the following:
  - **UNC path**: type the path where the source file exists.
  - **Username** and **Password**: type the username and password if the source location requires authentication.

Manually Updating a local AU server

If the Server/Device is updated through a Local AutoUpdate Server, but the Management Server cannot connect to the Internet; then, manually update the local AU Server before doing a Server/Device Update.

Procedure

1. Obtain the installation package from your Trend Micro representative.
2. Extract the installation package.
3. Copy the folders to the local AutoUpdate Server.

Note

When using a local AutoUpdate Server, you should check for updates periodically.

Chapter 9

Viewing and Maintaining Logs

This chapter shows you how to view logs on the Mobile Security administration web console and configure log deletion settings.

The chapter includes the following sections:

- *About Logs on page 9-2*
- *Viewing Mobile Device Agent Logs on page 9-2*
- *Log Maintenance on page 9-4*

About Logs

Mobile Security maintains the following types of logs:

- **Administrator logs**: When an administrator performs any configuration on the administrator web console, Mobile Security generates a log on the Management Server.
- **Mobile Device Agent logs**: When Mobile Device Agents generate an application scan log, device vulnerability log, network protection log or Web threat protection log, the log is sent to the Mobile Security Management Server. This enables Mobile Device Agent logs to be stored on a central location so you can assess your organization's protection policies and identify mobile devices at a higher risk of infection or attack.

Viewing Mobile Device Agent Logs

You can view Mobile Device Agent logs on mobile devices or view all Mobile Device Agent logs on Mobile Security Management Server. On the Management Server, you can view the following Mobile Device Agent logs:

- Application Scan Logs: these logs are generated when Mobile Device Agent detects a malware, privacy threat, vulnerability risk, or a modified app on a mobile device.
- Device Vulnerability Logs: these logs are generated when the developer options or the USB debugging mode is enabled, or a malicious iOS profile is detected on a mobile device, or a rooted/jailbroken mobile device is detected.
- Network Protection Logs: these logs are generated when a network traffic decryption, a unsafe access point (Wi-Fi), or a malicious SSL certificate is detected on a mobile device.
- Web Threat Protection Logs: Mobile Device Agent generates a web threat protection log when it blocks a dangerous or malware-infected web page and then uploads the log to the server.

Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Notifications & Reports** > **Log Query**.

   The **Log Query** screen displays.

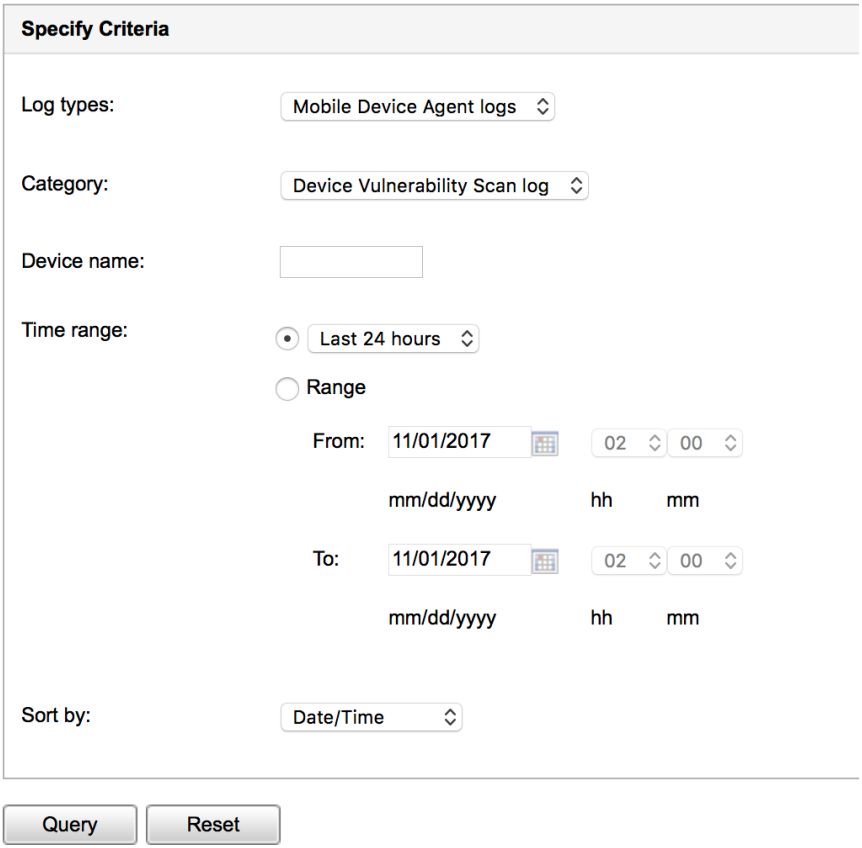


FIGURE 9-1. Log Query screen

3. Specify the query criteria for the logs you want to view. The parameters are:

- **Log types**—select the log type from the drop down menu.
- **Category**—select the log category from the drop down menu.
- **Administrator name** or **Device name**—type the administrator or device name whose related logs you want to search.
- **Time range**—select a predefined date range. Choices are: **All**, **Last 24 hours**, **Last 7 days**, and **Last 30 days**. If the period you require is not covered by the above options, select **Range** and specify a date range.
  - **From**—type the date for the earliest log you want to view. Click the icon to select a date from the calendar.
  - **To**—type the date for the latest log you want to view. Click the icon to select a date from the calendar.
- **Sort by**—specify the order and grouping of the logs.

4. Click **Query** to begin the query.

Log Maintenance

When Mobile Device Agents generate event logs about security risk detection, the logs are sent and stored on the Mobile Security Management Module. Use these logs to assess your organization's protection policies and identify mobile devices that face a higher risk of infection or attack.

To keep the size of your Mobile Device Agent logs from occupying too much space on your hard disk, delete the logs manually or configure Mobile Security administration web console to delete the logs automatically based on a schedule in the Log Maintenance screen.

Scheduling Log Deleting

Procedure

1. Click **Notifications & Reports** > **Log Maintenance**.

   The **Log Maintenance** screen displays.

2. Select **Enable scheduled deletion of logs**.

3. Select the log types to delete.

4. Select whether to delete logs for all the selected log types or those older than the specified number of days.

5. Specify the log deletion frequency and time.

6. Click **Save**.

Deleting Logs Manually

Procedure

1. Click **Notifications & Reports** > **Log Maintenance**.

   The **Log Maintenance** screen displays.

2. Select the log types to delete.

3. Select whether to delete logs for all the selected log types or only older than the specified number of days.

4. Click **Delete Now**.

Chapter 10

Using Notifications and Reports

This chapter shows you how to configure and use notifications and reports in Mobile Security.

The chapter includes the following sections:

- *About Notification Messages and Reports on page 10-2*
- *Configuring Notification Settings on page 10-2*
- *Configuring Email Notifications on page 10-2*
- *Administrator Notifications on page 10-3*
- *Reports on page 10-4*
- *User Notifications on page 10-9*

About Notification Messages and Reports

You can configure Mobile Security to send notifications and reports via email to the administrator(s) and/or users.

- **Administrator Notifications**—sends email notifications to the administrator in case any system abnormality occurs.
- **Reports**—sends reports to the specified email recipients.
- **User Notifications**—sends email and/or a text message to notify mobile devices to download and install Mobile Device Agent.

Configuring Notification Settings

Configuring Email Notifications

If you want to send email message notifications to the users, then you must configure these settings.

Procedure

1. Click **Notifications & Reports** > **Settings**.

   The **Notifications & Reports Settings** screen displays.

2. Under **Email Settings** section, type the **From** email address, the SMTP server IP address and its port number.

3. If the SMTP server requires authentication, select **Authentication**, and then type the username and password.

4. Click **Save**.

Administrator Notifications

Use the **Administrator Notifications** screen to configure the following:

- **Real-time Malware Detection Warning**—sends email notification to administrator when the agent detects a malware.
- **Malicious Certificate Warning**—sends email notification to administrator when the agent detects a malicious certificate.
- **Malicious iOS Profile Warning**—sends email notification to administrator when the agent detects a malicious iOS profile.
- **System Error**—sends email notification to the administrator in case any system abnormality occurs. Token variables `<%PROBLEM%>`, `<%REASON%>` and `<%SUGGESTION%>` will be replaced by the actual problem, reason and the suggestion to resolve the problem.
- **APNS Certificate Expired Warning**—sends email notification to administrator one month before the APNs certificate expires.

Enabling Administrator Notifications

Procedure

1. Go to **Notifications & Reports** > **Administrator Notifications**.

   The **Administrator Notifications** screen displays.

2. Select the notifications and reports you want to receive via email.
3. Click **Save**.

Configuring Administrator Notification Settings

Procedure

1. Go to **Notifications & Reports** > **Administrator Notifications**.

   The **Administrator Notifications** screen displays.

2. Under **Notification Settings**, click a notification name.

   The **Email Settings** screen of the selected notification appears.

3. Update the following as required:

   - **To**: Email address of the administrator.

     Note

     Use a semicolon ";" to separate multiple email addresses.

   - **Subject**: Subject line of the notification email.
   - **Message**: Message body of the notification .

4. Click **Save**.

Reports

Mobile Security allows you to generate and send the following reports:

- **Security Report**—displays information on detected malware, modified applications, privacy risks, vulnerable applications, network traffic decryption, unsafe access point (Wi-Fi), malicious SSL certificate, malicious iOS profile, developer options, USB debugging status, rooted/jailbreak status, and the top ten (10) blocked websites.
- **Devices Inventory Report**—displays comprehensive information on all managed devices.

- **Devices Enrollment Report**—displays information on device enrollment.

You can perform the following tasks from the **Reports** screen.

TABLE 10-1. Report Tasks

TASK	DESCRIPTION
Generate	You can generate new reports whenever you need them. For more information, see *Generating Reports on page 10-5*.
View	You can view the last generated reports from the On-Demand tab. For more information, see *Viewing Reports on page 10-6*.
Send	You can choose to send reports via email whenever needed. For more information, see *Sending Reports on page 10-7*.
Schedule	You can specify a fixed schedule for sending reports to administrators and other users. For more information, see *Scheduling Reports on page 10-8*.

Generating Reports

Note

Mobile Security only keeps one copy of each report type on the server.

Save a copy of the latest report before generating a new version.

Procedure

1. On the Mobile Security administration web console, go to **Notifications & Reports** > **Reports** > **On-Demand**.

   The **On-Demand** screen displays.

2. Select the time range.

- Today
- Last 7 days
- Last 30 days

3. Select all or one device platform.
   - All Types
   - iOS
   - Android
4. Select the user information to include in the report.
   - All
   - Specific
5. Select the reports that you want to generate.
6. Click **Generate**.

   Mobile Security generates the selected reports and overwrites all existing versions.

Viewing Reports

Procedure

1. On the Mobile Security administration web console, go to **Notifications & Reports** > **Reports**.
2. Locate the report you want to view from any of the following tabs.
   - **On-Demand**—Select to view on-demand reports.
   - **Scheduled**—Select to view scheduled reports.
3. Click **View**.

Note

If you do not see the link, you must first generate the report.

For more information, see *Generating Reports on page 10-5*

The selected report opens up in a new tab or window.

Sending Reports

Procedure

1. On the Mobile Security administration web console, go to **Notifications & Reports** > **Reports** > **On-Demand**.

   The **On-Demand** screen displays.

2. Locate the report you want from the **Report** table.

3. Click **Send**.

   Note

   If you do not see the link, you must first generate the report.

   For more information, see *Generating Reports on page 10-5*

   The **Send Report** screen appears.

4. Type the email address of the recipient.

5. You can choose to modify the email subject and message.

6. Click **Send**.

   A confirmation message appears.

Scheduling Reports

Procedure

1. On the Mobile Security administration web console, go to **Notifications & Reports** > **Reports** > **Scheduled**.

   The **Scheduled** screen displays.

2. Select the report frequency from the drop-down list.

   - **Daily**
   - **Weekly**: Specify the day of the week when the report will be sent out using the drop-down list.
   - **Monthly**: Specify the day of the month when the report will be sent out using the drop-down list.

3. Click **Save**.

Modifying the Email Template

Procedure

1. On the Mobile Security administration web console, go to **Notifications & Reports** > **Reports** > **Scheduled**.

   The **Scheduled** screen displays.

2. Click a report name.

   The **Email Settings** screen of the selected report appears.

3. Update the following as required:

   - **To**: Email address of the administrator.

Note

Use a semicolon ";" to separate multiple email addresses.

- **Subject**: Subject line of the report email.
- **Message**: Message body of the report.

4. Click **Save**.

   A confirmation message appears.

User Notifications

Use the **User Notifications** screen to configure the following email message notification:

- **Mobile Device Enrollment**—sends email and/or a text message to notify mobile devices to download and install Mobile Device Agent. Token variable <%DOWNLOADURL%> will be replaced by the actual URL of the setup package.

Configuring User Notifications

Procedure

1. Click **Notifications & Reports** > **User Notifications**.

   The **User Notifications** screen displays.

2. Select the notifications you want to send to user via email or text message, and then click on individual notifications to modify their contents.

   - To configure email notification messages, update the following details as required:

- **Subject**: The subject of the email message.
- **Message**: The body of the email message.

- To configure text notification messages, update the body of the message in the **Message** field.

3. Click **Save** when done, to return back to the **User Notifications** screen.

Chapter 11

Technical Support

Learn about the following topics:

- *Troubleshooting Resources on page 11-2*
- *Contacting Trend Micro on page 11-3*
- *Sending Suspicious Content to Trend Micro on page 11-4*
- *Other Resources on page 11-5*

Troubleshooting Resources

Before contacting technical support, consider visiting the following Trend Micro online resources.

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to https://success.trendmicro.com.
2. Select from the available products or click the appropriate button to search for solutions.
3. Use the **Search Support** box to search for available solutions.
4. If no solution is found, click **Contact Support** and select the type of support needed.

   Tip

   To submit a support case online, visit the following URL:

   https://success.trendmicro.com/smb-new-request

   A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Threat Encyclopedia

Most malware today consists of blended threats, which combine two or more technologies, to bypass computer security protocols. Trend Micro combats this complex malware with products that create a custom defense strategy.

The Threat Encyclopedia provides a comprehensive list of names and symptoms for various blended threats, including known malware, spam, malicious URLs, and known vulnerabilities.

Go to https://www.trendmicro.com/vinfo/us/threat-encyclopedia/#malware to learn more about:

- Malware and malicious mobile code currently active or "in the wild"
- Correlated threat information pages to form a complete web attack story
- Internet threat advisories about targeted attacks and security threats
- Web attack and online trend information
- Weekly malware reports

Contacting Trend Micro

In the United States, Trend Micro representatives are available by phone or email:

Address	Trend Micro, Incorporated 225 E. John Carpenter Freeway, Suite 1500 Irving, Texas 75062 U.S.A.
Phone	Phone: +1 (817) 569-8900 Toll-free: (888) 762-8736
Website	https://www.trendmicro.com
Email address	support@trendmicro.com

- Worldwide support offices:

  https://www.trendmicro.com/us/about-us/contact/index.html

- Trend Micro product documentation:

https://docs.trendmicro.com

Speeding Up the Support Call

To improve problem resolution, have the following information available:

- Steps to reproduce the problem
- Appliance or network information
- Computer brand, model, and any additional connected hardware or devices
- Amount of memory and free hard disk space
- Operating system and service pack version
- Version of the installed agent
- Serial number or Activation Code
- Detailed description of install environment
- Exact text of any error message received

Sending Suspicious Content to Trend Micro

Several options are available for sending suspicious content to Trend Micro for further analysis.

Email Reputation Services

Query the reputation of a specific IP address and nominate a message transfer agent for inclusion in the global approved list:

https://servicecentral.trendmicro.com/en-us/ers/

Refer to the following Knowledge Base entry to send message samples to Trend Micro:

https://success.trendmicro.com/solution/1112106

File Reputation Services

Gather system information and submit suspicious file content to Trend Micro:

https://success.trendmicro.com/solution/1059565

Record the case number for tracking purposes.

Web Reputation Services

Query the safety rating and content type of a URL suspected of being a phishing site, or other so-called "disease vector" (the intentional source of Internet threats such as spyware and malware):

https://global.sitesafety.trendmicro.com/

If the assigned rating is incorrect, send a re-classification request to Trend Micro.

Other Resources

In addition to solutions and support, there are many other helpful resources available online to stay up to date, learn about innovations, and be aware of the latest security trends.

Download Center

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to a specific product or service. To find out whether any patches are available, go to:

https://www.trendmicro.com/download/

If a patch has not been applied (patches are dated), open the Readme file to determine whether it is relevant to your environment. The Readme file also contains installation instructions.

Documentation Feedback

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please go to the following site:

https://docs.trendmicro.com/en-us/survey.aspx

Index

A

administration web console, 2-2, 2-4
- operations, 2-2
- URL, 2-2
- username and password, 2-3

administrator logs
- about, 9-2

C

command statuses, 2-18
Compatibility View, 2-4
component updates
- about, 8-2
- download sources, 8-4
- local AU server, 8-5
- scheduled, 8-3

D

device detection logs
- log types, 9-2

documentation feedback, 11-6

F

Full license version, 2-4

M

Managed Devices tab, 4-2
MDA logs
- about, 9-2
- Application Scan Logs, 9-2
- Device Vulnerability Logs, 9-2
- log types, 9-2
- Network Protection Logs, 9-2
- query criteria, 9-3
- Web Threat Protection Logs, 9-2

mobile device authentication, 1-15
Mobile Security
- about, 1-2
- Active Directory, 1-4
- architecture, 1-3
- Basic Security Model, 1-3
- certificate
  - authority, 1-5
  - management, 2-20
  - public and private keys, 1-5
  - SCEP, 1-5
  - security credentials, 1-5
  - SSL certificate, 1-5
- Cloud Communication Server, 1-4
- communication methods, 1-3
- Communication Server, 1-4
- Communication Server types, 1-4
- components, 1-3
- deployment models, 1-3
- encryption software compatibility, 1-2
- Enhanced Security Model
  - Cloud Communication Server, 1-3
  - Local Communication Server, 1-3
- Local Communication Server, 1-4
- Management Server, 1-4
- Microsoft SQL Server, 1-4
- Mobile Device Agent, 1-4
- OfficeScan, 1-2
- SMTP server, 1-5
- sub-groups, 4-2

unwanted network communications, 1-2
mobile threats, 1-2
spam messages, 1-2

N

notifications, 10-3
notifications and reports
about, 10-2
email message configuration, 10-9
token variables, 10-9

R

regular updates, 1-16
reports, 10-4
root account properties, 2-11

S

security scanning, 1-15
Super Administrator role properties, 2-12
support
resolve issues faster, 11-4

U

updating device information, 4-10
user account details, 2-14

W

what's new
v9.6, 1-14
v9.6 SP1, 1-13
v9.7, 1-12
v9.7 Patch 2, 1-11
v9.7 Patch 3, 1-11
v9.8, 1-10
v9.8 sp1, 1-10
v9.8 sp2, 1-9
v9.8 sp2 Patch 1, 1-9
v9.8 sp3, 1-8
v9.8 sp4, 1-8
v9.8 sp5, 1-7
v9.8 sp5 critical patch 1, 1-7
v9.8 sp5 critical patch 2, 1-7
v9.8 sp5 critical patch 3, 1-6

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736
Email: support@trendmicro.com

www.trendmicro.com

Item Code: TSEM99590/220830