Trend Micro™ Mobile Security 9.8

Service Pack 5 Critical Patch 6

Administrator's Guide

(for Full Version Deployment Mode)

Comprehensive security for enterprise handhelds

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 © 2023. Trend Micro Incorporated. All rights reserved.

Document Part No.: TSEM909723/230410

Release Date: August 2023

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 1

Audience 2

Mobile Security Documentation 2

Document Conventions 3

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 1-7

What's New in Release 9.8 SP5 Critical Patch 6 1-7

What's New in Release 9.8 SP5 Critical Patch 5 1-7

What's New in Release 9.8 SP5 Critical Patch 4 1-8

What's New in Release 9.8 SP5 Critical Patch 3 1-8

What's New in Release 9.8 SP5 Critical Patch 2 1-8

What's New in Release 9.8 SP5 Critical Patch 1 1-9

What's New in Release 9.8 SP5 1-9

What's New in Release 9.8 SP4 1-10

What's New in Release 9.8 SP3 1-10

What's New in Release 9.8 SP2 Patch 1 1-10

What's New in Release 9.8 SP2 1-11

What's New in Release 9.8 SP1 1-11
What's New in Release 9.8 1-11
What's New in Release 9.7 Patch 3 1-12
What's New in Release 9.7 Patch 2 1-13
What's New in Release 9.7 1-13
What's New in Release 9.6 SP1 1-14
What's New in Release 9.6 1-15
Main Mobile Device Agent Features 1-16
Supported Mobile Device OS Features 1-18

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 2-8
Adding a New Tab 2-9
Removing a Tab 2-9
Adding Widgets 2-9
Removing Widgets 2-10
Changing Widget's Position 2-10
Refreshing the Information on the Widgets 2-10
Viewing or Modifying Tab Settings 2-11
Administration Settings 2-11
Configuring Active Directory (AD) Settings 2-11
Configuring User Authentication 2-11
Configuring Database Settings 2-11
Configuring Communication Server Settings 2-11
Configuring Deployment Settings 2-12
Switching from Full Version to Security Scan Deployment Mode 2-12

Managing Administrator Accounts 2-12
Default Administrator Account Name and Role 2-12
Adding Administrator Accounts 2-15
Editing an Administrator Account 2-16
Deleting an Administrator Account 2-17
Creating an Administrator Role 2-17
Editing an Administrator Role 2-18
Deleting an Administrator Role 2-18
Changing Administrator Password 2-18
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
Exchange Server Integration 2-21
Configuring Exchange Server Integration Settings 2-21
Configuring Exchange Connector 2-21
Transferring to a New Exchange Server 2-22

Chapter 3: Managing Mobile Devices

Managed Devices Tab 3-2
Groups in Mobile Security 3-2
Managing Groups 3-3
Adding a Group 3-3
Renaming a Group 3-4
Deleting a Group 3-4
Managing Mobile Devices 3-4
Reassigning Devices 3-5
Editing Mobile Device Information 3-5
Deleting Mobile Devices 3-6
Deleting Single Mobile Device 3-6
Deleting Multiple Mobile Devices 3-7
Moving Mobile Devices to Another Group 3-7

Mobile Device Status 3-8
Basic Mobile Device Agent Search 3-9
Advanced Mobile Device Agent Search 3-9
Mobile Device Agent Tasks 3-10
Updating Mobile Device Agents 3-10
Updating Mobile Device Information 3-11
Lost Device Protection 3-12
Locating a Remote Mobile Device 3-12
Locking a Remote Mobile Device 3-13
Wiping a Remote Mobile Device 3-14
Resetting Password Remotely 3-15
Resetting Password for an Android Mobile Device ... 3-15
Removing the Password for an iOS Mobile Device ... 3-16
Managing Samsung KNOX Workspace Remotely 3-16
Modifying iOS Settings Remotely 3-17
Exporting Data 3-18
Sending Messages to Mobile Devices 3-19
Exchange ActiveSync Devices Tab 3-19
Inviting Exchange ActiveSync Users 3-20
Allowing or Blocking Access to Exchange Server 3-21
Wiping a Remote ActiveSync Mobile Device 3-21
Removing an ActiveSync Mobile Device 3-22
Device Enrollment Program Tab 3-23
Device Enrollment Program User Experience 3-23
Setting Up Mobile Security for the Device Enrollment Program 3-24
Integration with Trend Micro Control Manager 3-26
Creating Security Policies in Control Manager 3-27
Deleting or Modifying Security Policies 3-27
Security Policy Statuses on Control Manager 3-27

Chapter 4: Managing Users and Invitations

Users Tab 4-2
Viewing the Users List 4-2

Inviting a User Again 4-3
Editing User Information 4-3
Deleting a User 4-4
Invitations Tab 4-4
Viewing the Invitations List 4-5
Resending Invitations 4-5
Canceling Active Invitations 4-6
Removing Invitations from the List 4-6

Chapter 5: Protecting Devices with Policies

About Policies 5-2
Policies for All Devices 5-3
Application Approved List 5-3
Trusted Network Traffic Decryption Certificate List 5-4
Managing Policies for All Devices 5-4
Adding Applications to Approved List 5-4
Removing Applications from Approved List 5-5
Adding a Trusted Network Traffic Decryption Certificate 5-6
Deleting a Trusted Network Traffic Decryption Certificate 5-6
Policies for All Groups 5-7
Common Policy 5-7
Wi-Fi Policy 5-8
Exchange ActiveSync Policy 5-8
VPN Policy 5-8
Global HTTP Proxy Policy 5-8
Certificate Policy 5-9
Single Sign-On Policy 5-9
AirPlay/AirPrint Policy 5-10
Cellular Network Policy 5-10
Theme Policy 5-10
Managed Domains Policy 5-10
Security Policy 5-11

Spam Prevention Policy 5-14
Spam SMS Prevention Policies 5-14
Spam WAP Push Prevention Policies 5-16
Call Filtering Policy 5-18
Password Policy 5-20
Feature Lock Policy 5-20
Compliance Policy 5-21
Application Monitor and Control Policy 5-21
Volume Purchasing Program Policy 5-24
Container Policy 5-24
Managing Policies for All Groups 5-25
Creating a Policy 5-26
Editing a Policy 5-26
Assigning or Removing Policy from a Group 5-27
Copying a Policy 5-27
Deleting Policies 5-28
Configuring Application Availability 5-28

Chapter 6: Managing Applications

About the Enterprise App Store 6-2
Managing Enterprise Apps 6-2
Adding an Application 6-2
Editing Application Information 6-4
Deleting Applications from the App Store 6-4
Managing Application Categories 6-5
Adding an Application Category 6-5
Editing an Application Category 6-5
Deleting an Application Category 6-6
Managing Apps Purchased through the Volume Purchase Program 6-6
Setting Up Volume Purchase Program Licenses 6-7
Assigning or Reclaiming VPP Licenses 6-7
Checking Status for VPP Users 6-9
Reclaiming All Licenses from a User 6-10
About Installed Apps 6-10
Viewing Installed Applications 6-11

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 7-5
Viewing Malicious iOS Profiles 7-6

Chapter 8: Viewing and Maintaining Logs

About Logs 8-2
Viewing Mobile Device Agent Logs 8-2
Log Maintenance 8-5
Scheduling Log Deleting 8-5
Deleting Logs Manually 8-6

Chapter 9: Using Notifications and Reports

About Notification Messages and Reports 9-2
Configuring Notification Settings 9-2
Configuring Email Notifications 9-2
Configuring SMS Sender Settings 9-2
SMS Sender List 9-3
Configuring SMS Sender List 9-4
Monitoring SMS Senders 9-5
Editing an SMS Sender 9-5
Deleting an SMS Sender 9-5
Handling SMS Sender Client App 9-6
Setting up SMS Sender Client App 9-6
Stopping SMS Sender 9-6
SMS Sender Status 9-6
Viewing SMS Sender History 9-7
Viewing SMS Sender Running Logs 9-7
Administrator Notifications 9-7
Enabling Administrator Notifications 9-8
Configuring Administrator Notification Settings 9-8

Reports 9-9
Generating Reports 9-10
Viewing Reports 9-11
Sending Reports 9-12
Scheduling Reports 9-12
Modifying the Email Template 9-13
User Notifications 9-14
Configuring User Notifications 9-14

Chapter 10: Updating Components

About Component Updates 10-2
Updating Mobile Security Components 10-2
Manual Update 10-2
Scheduled Update 10-3
Specifying a Download Source 10-4
Manually Updating a local AU server 10-5

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 11-3
Sending Suspicious Content to Trend Micro 11-4
Email Reputation Services 11-4
File Reputation Services 11-4
Web Reputation Services 11-5
Other Resources 11-5
Download Center 11-5
Documentation Feedback 11-5

Index

Index IN-1

Preface

Preface

Welcome to the Trend Micro™ Mobile Security for Enterprise version 9.8 SP5 Critical Patch 6 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 2*
- *Mobile Security Documentation on page 2*
- *Document Conventions on page 3*

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
Note	Configuration notes

Convention	Description
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 6 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*
- *Comparison Between Local and Cloud Communication Servers on page 1-7*
- *What's New in Release 9.8 SP5 Critical Patch 3 on page 1-8*
- *Main Mobile Device Agent Features on page 1-16*
- *Supported Mobile Device OS Features on page 1-18*

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. Some of these unwanted network communications include: SMS messages, WAP push mails and data received through 3G/GPRS connections.

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 and SMS management, are possibly 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 1-7*.	Required
SMS Senders	You can use SMS Sender to send SMS text messages to the users.	Optional

Component	Description	Required or Optional
Exchange Connector	Trend Micro Mobile Security uses Exchange Connector to communicate with the Microsoft Exchange server, detects all the mobile devices that use Exchange ActiveSync service, and displays them on Mobile Security web console. The Microsoft Exchange server Integration with Mobile Security enables the administrators to monitor the mobile devices that access the Microsoft Exchange server. Once the feature is enabled and configured, Mobile Security administrators can perform Remote Wipe and block the access to the Microsoft Exchange server for such mobile devices. The integration of Microsoft Exchange server with Mobile Security also enables the administrators to control the user access to cooperate data (such as, emails, calendar, contacts, and so on).	Optional
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
Certificate Authority	The Certificate Authority manages security credentials and public and private keys for secure communication.	Optional

Component	Description	Required or 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
APNs Certificate	(**Full Version** deployment mode, and **Security Scan** deployment mode with unlisted MDM vendor only.) The Mobile Security Communication Server communicates through the Apple Push Notification Service (APNs) to iOS devices.	Required, if you want to manage iOS mobile devices
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 6

The following new features are available in Trend Micro Mobile Security 9.8 SP5 Critical Patch 6:

FEATURE	DESCRIPTION
Security Vulnerability Fix	This version of Mobile Security resolves a few Cross-Site Scripting vulnerabilities found in the web console module.

What's New in Release 9.8 SP5 Critical Patch 5

The following new features are available in Trend Micro Mobile Security 9.8 SP5 Critical Patch 5:

FEATURE	DESCRIPTION
Security Vulnerability Fix	This version of Mobile Security resolves a potential unauthenticated file deletion issue and a potential information disclosure issue on the Management Server.

What's New in Release 9.8 SP5 Critical Patch 4

The following new features are available in Trend Micro Mobile Security 9.8 SP5 Critical Patch 4:

Feature	Description
Security Vulnerability Fix	This version of Mobile Security resolves an authentication bypass vulnerability and a remote code execution vulnerability in the administration web console.
Incorrect Malware Pattern Version Number	This version of Mobile Security resolves the incorrect malware pattern version number in the exported mobile device information file.

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.
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 SP4:

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 SP4 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.
PHP Version Upgrade	This version of Mobile Security upgrades Trend Micro Mobile Security built-in PHP version from 5.4.38 to 7.0.33.
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
Update of MARS Pattern Tool	This version of Mobile Security updates the MARS pattern tool and catches logs if the MARS pattern version fails to upgrade.

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.

What's New in Release 9.8

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

Feature	Description
Integration with Trend Micro Control Manager (TMCM) 7.0	Supports full integration with TMCM 7.0.
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
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.

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.

Feature	Description
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.

Feature	Description
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.
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.

Feature	Description
Report Generation by Device Platform	Enhancements to the report generation feature allow administrators to generate reports for selected device platforms.
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	●	

Feature Name	Description		Android	iOS
Web Security	As technology increases for mobile devices, the sophistication of mobile threats is also increasing. Trend Micro Mobile Security provides Web Reputation and Parental Controls to protect your mobile device from unsafe websites and the websites that may contain objectionable material for children, teenagers and other family members. You can modify your Web Reputation and Parental Controls setting levels as per your desired settings. Mobile Security also maintains the log of the websites that were blocked by Web Reputation or Parental Controls in their specific logs.		●	
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.		●	●
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	●	●
		Policy violation logs	●	●
		Device vulnerability logs	●	●
		Network protection logs	●	●

Feature Name	Description		Android	iOS
		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	●	
		Call blocking history	●	
		Text blocking history	●	
		Update 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 6 Feature Matrix

Category	Features	Settings			Requirements
Common		Disallow Mobile Security Agent uninstallation		●	For Android: supported only on Android 5, 6, and 7

CATEGORY	FEATURES	SETTINGS			REQUIREMENTS
		Allow Mobile Security client configuration		●	
Provisioning	Wi-Fi	Standard Wi-Fi configuration	●	●	For Android: supported only on Android 5, 6, 7, 8, and 9
		Legacy hotspot configuration	●		
		Hotspot 2.0 configuration	●		
	Exchange ActiveSync	Exchange ActiveSync configuration	●		
	VPN	VPN configuration	●		
	Global HTTP Proxy	Global HTTP Proxy configuration	●		
	Single Sign-on	Single sign-on configuration	●		
	Certificate	Certificate configuration	●		
	Cellular network	Cellular network configuration	●		
	AirPlay/ AirPrint	AirPlay/AirPrint configuration	●		
	Themes (Supervised only)	Wallpaper configuration	●		
		Font configuration	●		

Category	Features	Settings			Requirements
	Managed Domains	Unmarked Email Domains	●		
		Managed Safari Web Domains	●		
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		●	
Data Protection	Password Settings	Use password for login	●	●	
		Allow simple password	●	●	
		Require alphanumeric password	●	●	
		Minimum password length	●	●	
		Password expiration	●	●	
		Password history	●	●	

CATEGORY	FEATURES	SETTINGS			REQUIREMENTS
		Auto-lock	●	●	
		Password failure action	●	●	
	Feature Lock	Camera	●	●	For Android: supported only on Android 5, 6, 7, 8, and 9
		FaceTime (Supervised only)	●		
		Screen capture	●		
		Apps installation	●		
		Sync while roaming	●		
		Voice dialing	●		
		In-app purchase	●		
		Multiplayer gaming	●		
		Adding game center friends	●		
		Game Center (Supervised Only)	●		
		Force encrypted backups	●		
		Explicit music, podcast and iTunes U	●		
		Passbook while device is locked	●		

Category	Features	Settings			Requirements
		Bluetooth and Bluetooth discovery		●	For Android: On some devices, supported only when consented by end users
		WLAN/Wi-Fi		●	For Android: supported only on Android 5, 6, 7, 8, and 9
		3G data network		●	
		Developer mode		●	
		Speaker/ speakerphone/ microphone			
		Restrict memory cards (Supervised only)		●	
		Siri (Supervised only)	●		
		Siri while device is locked (Supervised only)	●		
		Enable profnity filter (Supervised only)	●		
		Enable access to iCloud services (Supervised only)	●		
		Cloud backup (Supervised only)	●		

Category	Features	Settings			Requirements
		Cloud document sync (Supervised only)	●		
		Photo Stream (Supervised only)	●		
		Shared Photo Streams (Supervised only)	●		
		Diagnostic data (Supervised only)	●		
		Accept untrusted Transport Layer Security (TLS)	●		
		Force iTunes to store password	●		
		Open documents from managed apps in other apps	●		
		Open documents from other apps in managed apps	●		
		iTunes	●		
		Safari Web browser	●		
		AutoFill	●		
		JavaScript	●		
		Popups	●		
		Force fraud warning	●		
		Accept cookies	●		

Category	Features	Settings			Requirements
		Removing apps (Supervised only)	●		
		Bookstore (Supervised only)	●		
		Erotica (Supervised only)	●		
		Configuration Profile Installation (Supervised only)	●		
		iMessage (Supervised only)	●		
		Ratings region	●		
		Movies	●		
		TV Shows	●		
		Apps	●		
		Account modification (Supervised only)	●		
		AirDrop (Supervised only)	●		
		Applications cellular data modification (Supervised only)	●		
		Assistant (Siri) user-generated content (Supervised only)	●		
		Cloud keychain synchronization	●		

Category	Features	Settings			Requirements
		Find My Friends modification (Supervised only)	●		
		Fingerprint for unlocking a device	●		
		Host pairing (Supervised only)	●		
		Lock screen control center	●		
		Lock screen notifications view	●		
		Lockscreen today view	●		
		Over the Air Public Key Infrastructure (OTAPKI) updates	●		
		Force limit ad tracking	●		
		Force AirPlay outgoing requests pairing password	●		
		Allow managed apps to store data in iCloud	●		
		Allow backup of enterprise books	●		
		Allow configuration restrictions	●		
		Allow Erase All Content and Settings	●		

Category	Features	Settings			Requirements
		Allow Handoff	●		
		Allow Internet results in spotlight	●		
		Allow notes and highlights sync for enterprise books	●		
		Allow sharing of managed documents using AirDrop	●		
		Allow iCloud Photo Library	●		
		Allow installing apps from device	●		
		Allow keyboard shortcuts	●		
		Allow paired Apple Watch	●		
		Allow passcode modification	●		
		Allow device name modification	●		
		Allow wallpaper modification	●		
		Allow automatic downloading of apps	●		
		Allow trusting of enterprise apps	●		
		Access point		●	For Android: supported only

Category	Features	Settings			Requirements
					on Android 5, 6, 7, 8, and 9
	Compliance Settings	Rooted/Jailbroken	●	●	
		Unencrypted	●	●	
		OS version check	●	●	
Application Management	Application Monitor & Control	Required Applications	●	●	
		Permitted Applications	●	●	
		Lock to App (Supervised only)	●		
	Volume Purchasing Program	Volume Purchasing Program	●		
Remote Control	Register		●	●	
	Update		●	●	
	Anti-theft	Remote locate	●	●	
		Remote lock	●	●	
		Remote wipe	●	●	
		Reset password	●	●	For Android: supported only on Android 5 and 6
		Send message	●	●	
	Samsung KNOX Workspace	Create container		●	
		Remove container		●	

CATEGORY	FEATURES	SETTINGS			REQUIREMENTS
		Lock container		●	
		Unlock container		●	
		Reset container password		●	
Samsung KNOX Workspace Policy	Container account setting	Blocked list		●	
		Approved list		●	
	Restriction settings	Allow users to use camera		●	
		Allow display the share via list of applications		●	
	Browser settings	Enable auto fill setting		●	
		Enable cookies setting		●	
		Enable popups setting		●	
		Enable force fraud warning setting		●	
		Enable JavaScript setting		●	
		Enable Web Proxy		●	
Samsung KNOX Workspace Policy	Container password settings	Enable password visibility		●	
		Minimum password change length		●	
		Minimum password length		●	

CATEGORY	FEATURES	SETTINGS			REQUIREMENTS
		Maximum inactivity timeout		●	
		Maximum number of failed attempts		●	
		Password history		●	
		Maximum password age		●	
		Minimum number of special characters required in a password		●	
		Password complexity		●	
	Application settings	Installation approved list		●	
		Installation blocked list		●	
		Required applications		●	
		Disabled applications		●	
Device Enrollment Program			●		
Device information	Hardware, Operating System	Serial Number	●	●	For Android: supported only on Android 5, 6, 7, and 8
		MEID	●	●	For Android: supported only on Android 5, 6, and 7

Category	Features	Settings			Requirements
		IMEI	●	●	For Android: supported only on Android 5, 6, and 7
		Industrial Design		●	For Android: supported only when mobile devices provide the information
		Bootloader Version		●	For Android: supported only when mobile devices provide the information
	Network	Bluetooth Mac	●	●	For Android: requires Android 7 or earlier to get the original MAC address. Android 8 or later reports a random address.
		Wi-Fi Mac	●	●	For Android: requires Android 7 or earlier to get the original MAC address. Android 8 or later reports a random address.

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 2-11*
- *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.

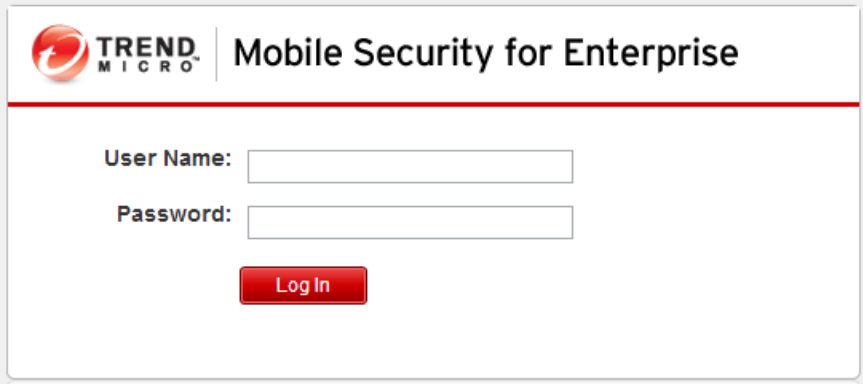

FIGURE 2-1. Administration Web console login screen

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

- View the total number of enrolled and unregistered mobile devices managed by Mobile Security.

  A mobile device may remain unregistered if a connection to the Communication Server is unsuccessful.

- View mobile device program patch and component update status:
  - **Current Version**—the current version number of the Mobile Device Agent or components on the Mobile Security Management Server
  - **Up-to-date**—the number of mobile device with updated Mobile Device Agent version or component
  - **Out-of-date**—the number of mobile devices that are using an out-of-date component
  - **Update Rate**—the percentage of mobile devices using the latest component version
  - **Upgraded**—the number of mobile devices using the latest Mobile Device Agent version
  - **Not Upgraded**— the number of mobile devices that have not upgraded to use the latest Mobile Device Agent version
  - **Upgrade Rate**—the percentage of mobile devices using the latest Mobile Device Agent
- View server update status:
  - **Server**—the name of the module
  - **Address**—the domain name or IP address of the machine hosting the module
  - **Current Version**—the current version number of the Mobile Security Management Server modules
  - **Last Updated**—the time and date of the last update

- **Compliance**—shows the app control, encryption and jailbreak/root status of mobile devices. In this category, you can:

- View the mobile device jailbreak/root status:
  - **Jailbroken/Rooted**—the number of mobile devices that are jailbroken/rooted
  - **Not Jailbroken/Rooted**—the number of mobile devices that are not jailbroken/rooted
- View the mobile device encryption status:
  - **Encrypted**—the number of mobile devices that are encrypted
  - **Not Encrypted**—the number of mobile devices that are not encrypted
- View the mobile device application control status:
  - **Compliant**—the number of mobile devices that comply with the Mobile Security's compliance and application control policy
  - **Not Compliant**—the number of mobile devices that do not comply with the Mobile Security's compliance and application control policy

- **Inventory**—shows mobile device operating system version summary, telephone carriers summary, mobile device vendors summary and top 10 applications installed on mobile devices.

Note

On each of the widgets on the **Dashboard** screen, you can either select **All**, or the group name from the drop-down list to display the information of the relevant devices.

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

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 2-16* 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 2-18* 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
Exchange Server Domain Control	Domain selection	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

Server Components	Permissions	Super Administrator	Group Administrator
	Exchange Server Integration	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
Applications	Enterprise App Store	Supported	Not supported
	Installed Apps	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
	Exchange ActiveSync Devices	Supported	Supported for managed groups only

Server Components	Permissions	Super Administrator	Group Administrator
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 2-16* 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**.

Exchange Server Integration

Configuring Exchange Server Integration Settings

Refer to the topic *Configuring Exchange Server Integration Settings* in the *Installation and Deployment Guide* for the detailed configuration steps.

Configuring Exchange Connector

You can configure the Exchange Connector to update automatically whenever a higher version is available.

Procedure

1. On the computer where Exchange Connector is installed, click the **Show hidden icons** button in the system tray on the Windows taskbar (near the system clock).
2. Right-click the **Exchange Connector** icon, and then click **About Trend Micro Mobile Security-Exchange Connector**.

   About Trend Micro Mobile Security-Exchange Connector screen appears.

3. Configure the following:

   - **Enable automatic upgrade**—when selected, the Exchange Connector automatically upgrades to a new version whenever it is available.
   - **Server Address**—Mobile Security Management Server IP address.
   - **HTTPS Port**—Mobile Security Management Server HTTPS port number for the administration web console.

Transferring to a New Exchange Server

To transfer to a new Exchange server, complete the following steps:

Procedure

1. Stop the existing Exchange Connector service on the computer where Exchange Connector is installed.
2. Log on to the Mobile Security administration web console.
3. Click **Administration** > **Exchange Server Integration**.
4. Click **Data Cleanup**.
5. Download and install the new Exchange Connector on the computer.

   For detailed information, see *Installation and Deployment Guide*.
6. Configure the Exchange Connector settings.

   See *Configuring Exchange Connector on page 2-21*.

Chapter 3

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 3-2*
- *Managing Groups on page 3-3*
- *Managing Mobile Devices on page 3-4*
- *Mobile Device Status on page 3-8*
- *Mobile Device Agent Tasks on page 3-10*
- *Updating Mobile Device Agents on page 3-10*
- *Integration with Trend Micro Control Manager on page 3-26*

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
- send a text message to mobile devices
- on-demand Mobile Device Agent component update, wipe/lock/locate remote 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 two sub-groups:

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

Note

- If you enable **Device Authentication** in **Device Enrollment Settings**, and upload a blank mobile device list for authentication, Mobile Security will move all the current enrolled mobile devices to the group "Unauthorized".
- **Device Authentication** supports Android and iOS mobile devices only.

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 3-6*
- *Deleting Multiple Mobile Devices on page 3-7*

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, firmware version information, and last iCloud backup.
- **Security**—displays the mobile device's statuses for encryption, 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; the connected access point (Wi-Fi), and the active iTunes account.
- **Network**—displays the Integrated Circuit Card ID (ICCID), Bluetooth and Wi-Fi MAC information, detailed network information including carrier network name, settings version, roaming status, Mobile Country Codes (MCC) and Mobile Network Codes (MNC) information, and personal hotspot status.

Note

USB Tethering Status and Bluetooth Tethering Status are no longer supported.

- **Policy**—shows the times the configuration and the security policy were last updated.
- **Installed Applications**—displays the list of all the applications that are installed on the mobile device, and the compliance check result. This tab is available only for Android and iOS mobile devices.

- **Samsung KNOX Information**—displays additional information about the mobile devices that support Samsung KNOX.

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
- **Mobile Device Agent Uninstalled by User**—confine the search to mobile devices on which Mobile Device Agent is uninstalled by the user
- **Rooted Mobile Device**—confine the search to rooted mobile devices
- **Infected mobile device agent**—confine the search to mobile devices with the specified number of detected malware
- **Device Status**—confine the search to the selected mobile devices' status(es)

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 10-2* 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**.

Lost Device Protection

If a user loses or misplaces the mobile device, you can remotely locate, lock or delete all of the data on that mobile device.

Locating a Remote Mobile Device

You can locate the mobile device through the wireless network or by using mobile device's GPS. The Management Server displays the mobile device location on Google Maps.

Note

This feature is available for Android and iOS mobile devices only.

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 locate.
4. Click **Device Locate** and then click **OK** on the confirmation dialog-box.

   The Mobile Security Management Server tries to locate the mobile device and displays the Google Maps link on the **Remote Locate Device** screen.
5. Click the Google Maps link on the **Remote Locate Device** screen to see the mobile device's most recent GPS location on the map.

Locking a Remote Mobile Device

You can send lock instruction from the administration web console to remotely lock a mobile device. Users will require to type the power-on password to unlock the mobile device.

Note

This feature is supported on Android and iOS mobile devices only.

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 lock.
4. Do one of the following:

   For an Android mobile device, click **Remote Lock** and then click **OK** on the confirmation dialog-box.

   For an iOS mobile device, click **Remote Lock** then type the user's phone number and a message that you want to send to the user, and then click **Lock**.

   The **Success** message displays on the screen if the lock command is generated successfully. To check whether the mobile device is locked successfully, you can check the command status in the **Command Queue Management** screen. See *Command Queue Management on page 2-18* for details.

Wiping a Remote Mobile Device

WARNING!

Be careful when you use this feature as the action CANNOT be undone. All data will be lost and irrecoverable.

You can remotely reset the mobile device to factory settings and clear the mobile device internal memory/SD card. This feature helps ensure the security of the data for lost, stolen or misplaced mobile devices. You can also choose to clear only the following corporate data on the mobile device:

- for Android: Exchange mail, calendar and contacts
- for iOS: MDM profiles, related policies, configurations and data

Note

This feature is supported on Android and iOS mobile devices only.

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 wipe.
4. Click **Remote Wipe**.

   The **Remote Wipe Device** screen displays.
5. Select the appropriate Device Name checkbox.
6. Do one of the following:
   - For Android mobile device, select one of the following:

- **Wipe all data to factory settings. (All applications and stored data will be removed. The inserted memory card will be formatted. This action cannot be undone.)**
- **Wipe email, calendar and contact list.**—also known as "selective wipe".

  If you select this option, you can also select **Wipe all data to factory settings if selective wipe failed.**.

- For iOS mobile device, select one of the following:
  - **Wipe all data to factory settings. (All applications and stored data will be removed. The inserted memory card will be formatted. This action cannot be undone.)**
  - **Wipe out all the provisioned profiles, policies, configurations, and its related data.**

7. Click **Remote Wipe Device**.

   The selected data is deleted from the mobile device and the Mobile Device Agent is unregistered from the server.

Resetting Password Remotely

If a user has forgotten the power-on password, you can remotely reset the password and unlock the mobile device from the Management Server. After the mobile device is successfully unlocked, the user is able to change the power-on password.

Note

This feature is supported on Android, and iOS mobile devices only.

Resetting Password for an Android 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. Select the mobile device from the tree, and then click **Password Reset**.

4. Type and confirm the new six-digit password on the pop-up dialog box that appears.

Removing the Password for an iOS 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. Select the mobile device from the tree, and then click **Password Reset**.

4. Click **OK** on the confirmation dialog box that appears. The power on password for the selected iOS mobile device will be removed.

Managing Samsung KNOX Workspace Remotely

You can send commands to manage Samsung KNOX workspaces from Mobile Security management web console. These commands include creating container, removing container, locking container, unlocking container, and resetting container password. This feature is available for Samsung mobile devices only.

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 Samsung mobile device from the device tree that you want to manage.

4. Do one of the following:

   - To create KNOX workspace on the mobile device, click **KNOX Operations** > **Create Container**.
   - To remove the workspace from the mobile device, click **KNOX Operations** > **Remove Container**.
   - To enable user to reset workspace password, click **KNOX Operations** > **Reset Password**.
   - To lock the workspace on the mobile device, click **KNOX Operations** > **Lock Container**.
   - To unlock the workspace on the mobile device, click **KNOX Operations** > **Unlock Container**.

Modifying iOS Settings Remotely

You can change the iOS mobile device settings remotely from the administration web console. These settings include data roaming, voice roaming, personal hotspot.

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 an iOS mobile device from the device tree that you want to manage.
4. Do one of the following:

   - To enable data roaming, click **iOS Operations** > **Enable Data Roaming**.
   - To disable data roaming, click **iOS Operations** > **Disable Data Roaming**.
   - To enable voice roaming, click **iOS Operations** > **Enable Voice Roaming**.

- To disable voice roaming, click **iOS Operations** > **Disable Voice Roaming**.
- To enable personal hotspot, click **iOS Operations** > **Enable Personal Hotspot**.
- To disable personal hotspot, click **iOS Operations** > **Disable Personal Hotspot**.
- To start Airplay mirroring, click **iOS Operations** > **Request AirPlay Mirroring**.
- To stop AirPlay mirroring, click **iOS Operations** > **Stop AirPlay Mirroring**.

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.

Sending Messages to Mobile Devices

You can send a text message to a user or a group from the **Managed Devices** tab in the **Devices** screen.

Note

When you send a text message to an iOS device, the information does not appear on the **Command Queue Management** screen.

Procedure

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

   The **Devices** screen displays.
3. From the device tree, select the mobile device or the device group to which you want to send a text message.
4. Click **Send Message**.

   The **Send a Text Message** screen appears.
5. Type your message in the field provided, and then click **Send**.

Exchange ActiveSync Devices Tab

After enabling the Exchange Server Integration on the Mobile Security Management Server, the **Exchange ActiveSync Devices** tab on **Devices** screen displays the list of mobile devices that connect to the Exchange Server through ActiveSync service.

On the **Exchange ActiveSync Devices** tab, you can perform the following actions:

- Allow or block access to Exchange Server
- On-demand remote wipe

- Cancel remote wipe command
- Remove mobile devices from the list

Note

The Mobile Security server matches mobile devices from the Exchange Server by device model and email address. For the devices enrolled with preset enrollment keys, the Mobile Security server may not be able to match them successfully from the Exchange Server.

Inviting Exchange ActiveSync Users

Before inviting Exchange ActiveSync users, make sure that you have configured the notifications and reports settings on the Management Server. Refer to the topic *Configuring Notifications & Reports Settings* in the *Installation and Deployment Guide*.

Procedure

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

   The **Devices** screen displays.
3. Click the **Exchange ActiveSync Devices** tab.
4. Select a mobile device assigned to the user that you want to invite to Mobile Security.
5. Click **Invite**, and then click **OK** on the confirmation screen that appears.

   Mobile Security sends an email message to the invited user. After the mobile device enrolls to the Mobile Security Management Server, the **Managed Device** column displays the status of the mobile device agent.

Allowing or Blocking Access to Exchange Server

Procedure

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

   The **Devices** screen displays.
3. Click the **Exchange ActiveSync Devices** tab.
4. Select a mobile device for which you want to allow or block access to Exchange Server.
5. Click **Allow Access** or **Block Access** and then click **OK** on the confirmation dialog box.

   The mobile device status in the **Exchange Access State** column displays the new status after the mobile device syncs with the Exchange Server.

Wiping a Remote ActiveSync Mobile Device

WARNING!

Be careful when you use this feature as the action CANNOT be undone. All data will be lost and unrecoverable.

You can remotely reset the ActiveSync mobile device to factory settings and clear the mobile device internal memory/SD card. This feature helps ensure the security of the data for lost, stolen or misplaced mobile devices.

For instructions on wiping a mobile device that does not use ActiveSync, see *Wiping a Remote Mobile Device on page 3-14*.

Procedure

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

The **Devices** screen displays.

3. Click the **Exchange ActiveSync Devices** tab.
4. Select the mobile device that you want to wipe.
5. Click **Remote Wipe**.

   The **Remote Wipe Device** screen pops up.
6. Select the device and then click **Remote Wipe Device**.

Removing an ActiveSync Mobile Device

The mobile device that you have remotely wiped from the Mobile Security Management Server will no longer be able to access the Exchange Server. You can remove such mobile device information from the **Exchange ActiveSync Devices** tab on the **Devices** screen.

Note

You can only remove mobile devices that are remotely wiped from the Mobile Security Management Server.

Procedure

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

   The **Devices** screen displays.
3. Click the **Exchange ActiveSync Devices** tab.
4. Select the mobile device that you want to remove from the list.
5. Click **Remove**, and then click **OK** on the confirmation screen.

Device Enrollment Program Tab

The Device Enrollment Program (DEP) provides a fast, streamlined way to deploy your corporate-owned iOS mobile devices. You can enroll your organization into the DEP program.

Trend Micro Mobile Security integrates with Apple Device Enrollment Program to streamline the enrollment of company-issued iOS 7 to iOS 11 mobile devices that are purchased directly from Apple. If you have configured the integration with the Device Enrollment Program, the users who are issued a corporate-owned iOS mobile devices are prompted to enroll with Mobile Security when they configure the mobile device using iOS activation process.

Integrating Mobile Security with DEP means that you do not need to communicate the enrollment instructions to the users, but still ensure that all the mobile devices are enrolled on the their first use. Additionally, this integration also removes the associated support cost.

Device Enrollment Program User Experience

If you configure Mobile Security integration with the Apple's Device Enrollment Program, the user experience is as follows:

- A user receives a new company-issued iOS mobile device, unpacks it, and switches it on.
- The mobile device connects to Apple.
- From the mobile device ID, the Apple servers detect that the device has been added to your Device Enrollment Program account and send device settings and connection details for your Mobile Security deployment.
- The user then uses the iOS Setup Assistant to complete the initial activation of the mobile device, which includes enrollment with Mobile Security.

You can determine the screens that appear in the iOS Setup Assistant when you configure integration with the Device Enrollment Program. This enables you to further streamline the activation process by skipping screens for settings that you configure through device management. For example, if you

plan to require that Location Services is enabled on the devices as part of a geo-fencing configuration, you can configure the iOS Setup Assistant to skip the screen that lets users choose whether to enable Location Services.

As part of the device activation process, the user is prompted to enroll with Mobile Security. The user does not need to enter credentials or an email address, and does not need to know connection details for Mobile Security. A specific Device Enrollment Program profile that admin creates automatically when you configure integration with the Device Enrollment Program is deployed to the device.

Setting Up Mobile Security for the Device Enrollment Program

Before you can configure Mobile Security for the Device Enrollment Program (DEP), make sure that you have already enrolled your organization to the DEP program on the following Apple website:

http://deploy.apple.com/

Procedure

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

   The **Devices** screen appears.
3. Click the **Device Enrollment Program** tab.
4. Click **Settings**.
5. Click the **Download** link before **Public Key** to download the public key to the local computer from Mobile Security Management Server.
6. Click the **Apple Deployment Programs** link before **Deployment**.

   The **Apple Deployment Programs** web portal opens in the Internet web browser.
7. Sign in to your **Device Enrollment Program** account and create a new MDM server using the public key you downloaded from the Mobile Security Management Server.

8. On the MDM server, generate an access token and save the token file to a suitable location, and then assign mobile devices for enrollment to the MDM server.

9. Upload the token file you generated through the **Apple Deployment Programs** web portal to the Mobile Security Management Server. Wait until the upload completes.

   After the upload completes, the **Device Enrollment Program Settings** screen appears.

10. Under the **Device Enrollment Program Detail** section, configure the following setup profile settings for mobile devices.

    - **Profile name**: a name for the setup profile displayed on the mobile device.
    - **Require supervision**: to place the mobile devices enrolled through the Device Enrollment Program to the supervised mode.
    - **Removable configuration**: to allow users to remove the device management configuration from devices enrolled through the Device Enrollment Program.
    - **Allow pairing**: to enable devices enrolled through the Device Enrollment Program to be managed through Apple tools such as iTunes and Apple Configurator.
    - **Mandatory configuration**: to prevent users from skipping the Mobile Security enrollment step in the device activation process.
    - **Business unit**: the name of the department to which the mobile device is assigned to.
    - **Unique service ID**: if you have multiple Mobile Security deployments, enter in the Unique service ID box a name that uniquely identifies the deployment you are configuring.
    - **Support phone number**: the phone number for users to call for assistance.
    - **Required setup items**: the setup items that are required for the users to configure. By default, all the setup items are required. If

you disable any of these items, the users will be able to skip that item during setup.

11. Under the **Enterprise Mobile Security Agent License** section, select the available option to assign Enterprise Mobile Security agent licenses to mobile devices. If Enterprise Mobile Security application exists in Volume Purchase Program, the application license will be assigned during enrollment through DEP. Otherwise, the licenes will be assigned using iTunes account.

Note

You must first configure **Volume Purchase Program Settings** to use this feature. Refer to the topic *Setting Up Volume Purchase Program Licenses on page 6-7* to configure Volume Purchase Program settings.

See topic *Installing MDA on Mobile Devices* in *Installation and Deployment Guide* for the procedure to deploy and enroll Enterprise Mobile Security MDA on iOS mobile devices through DEP.

12. Click **Save**.

    Mobile Security Management Server synchronizes the mobile device list with the Apple Device Enrollment Programs server and displays the mobile devices on the **Devices Enrollment Program** tab on **Devices** screen.

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 4

Managing Users and Invitations

This chapter shows you how to manage users and invitations lists in Mobile Security.

The chapter includes the following sections:

- *Users Tab on page 4-2*
- *Invitations Tab on page 4-4*

Users Tab

The **Users** tab enables you to perform the following tasks:

- invite a user to register
- invite a user again and change the assigned group
- edit user information
- delete a user
- search for a user

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.

Inviting a User Again

Note

This topic applies only to Mobile Security deployment in **Security Scan** mode with unlisted MDM solutions.

If your Mobile Security is integrated with AirWatch or MobileIron, this feature is disabled.

Procedure

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

   The **Users** screen displays.

2. Select the user and then click **Invite Again**

   The **Invite Again** screen appears.

3. Select the group from the drop-down list.

4. Click **Save**.

   A confirmation message appears.

Editing User Information

Procedure

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

   The **Users** screen displays.

2. Click the user name from the list.

   The **Edit User Information** screen appears.

3. Modify the user name and email address as required.

4. Click **Save**.

Mobile Security updates the user information.

Deleting a User

Note

You can only delete users without devices registered to the Mobile Security server.

Procedure

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

   The **Users** screen displays.

2. Select the user from the list and then click **Delete**.

3. On the confirmation message that appears, click **OK**.

   Mobile Security deletes the selected user.

Invitations Tab

The **Invitations** tab on the **Users** screen enables you to perform the following tasks:

- view the invitations list
- resend an invitation
- cancel an active invitation
- remove an invitation from the list
- search for an invitation

Viewing the Invitations List

Procedure

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

   The **Invitations** tab appears.

2. To filter the list, select the invitation status from the drop-down list.

Invitation Status	Description
Active	The invitation is valid and the user can use the information in the invitation message to enroll.
Expired	The invitation has expired and the user can no longer use the information in the invitation message to enroll.
Used	The user has already used the information in the invitation message to enroll and the Enrollment Key has become invalid. **Note** This status will only appear when the **Enrollment Key usage limitation option** is set to **Use for one time** in Device Enrollment Settings.
Canceled	The invitation is canceled from the server and the user cannot use the information in the invitation message to enroll.

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

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

Resending Invitations

Procedure

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

2. Select invitations from the list.
3. Click **Resend Invitation**.

   Mobile Security resends the invitation to the selected users.

Canceling Active Invitations

Procedure

1. On the Mobile Security administration web console, go to **Users** > **Invitations**
2. Select invitations from the list.
3. Click **Cancel Invitation**.

   The selected invitations are canceled.

Removing Invitations from the List

Note

You can only remove invitations with either **Used** or **Canceled** status.

Procedure

1. On the Mobile Security administration web console, go to **Users** > **Invitations**
2. Select invitations from the list.
3. Click **Remove Invitation**.

   The selected invitations are removed from the list.

Chapter 5

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 5-2*
- *Policies for All Devices on page 5-3*
- *Managing Policies for All Devices on page 5-4*
- *Policies for All Groups on page 5-7*
- *Managing Policies for All Groups on page 5-25*

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 5-1. Device Policies in Mobile Security

POLICY	REFERENCE
Approved List	See *Application Approved List on page 5-3*.
Trusted Network Traffic Decryption Certificate List	See *Trusted Network Traffic Decryption Certificate List on page 5-4*.

TABLE 5-2. Group Policies in Mobile Security

POLICY GROUP	POLICY	REFERENCE
General	Common Policy	See *Common Policy on page 5-7*.
Provisioning	Wi-Fi Policy	See *Wi-Fi Policy on page 5-8*.
	Exchange ActiveSync Policy	See *Exchange ActiveSync Policy on page 5-8*.
	Certificate Policy	See *Certificate Policy on page 5-9*.
	VPN Policy	See *VPN Policy on page 5-8*.
	Global HTTP Proxy Policy	See *Global HTTP Proxy Policy on page 5-8*.
	Single Sign-On Policy	See *Single Sign-On Policy on page 5-9*.
	Cellular Network Policy	See *Cellular Network Policy on page 5-10*.
	AirPlay/AirPrint Policy	See *AirPlay/AirPrint Policy on page 5-10*.
	Theme Policy	See *Theme Policy on page 5-10*.
	Managed Domains Policy	See *Managed Domains Policy on page 5-10*.

Policy Group	Policy	Reference
Device Security	Security Policy	See *Security Policy on page 5-11*.
	Spam Prevention Policy	See *Spam Prevention Policy on page 5-14*.
	Call Filtering Policy	See *Call Filtering Policy on page 5-18*.
Devices	Password Policy	See *Password Policy on page 5-20*.
	Feature Lock Policy	See *Feature Lock Policy on page 5-20*.
	Compliance Policy	See *Compliance Policy on page 5-21*.
Application Management	Application Monitor & Control Policy	See *Application Monitor and Control Policy on page 5-21*.
	Volume Purchasing Program Policy	See *Volume Purchasing Program Policy on page 5-24*.
Samsung KNOX	Container Policy	See *Container Policy on page 5-24*.

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** or **Applications** > **Installed Apps** on the menu bar.
     b. Click **Android** or **iOS** tab, and select the applications from the list of detected or installed 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** or **Applications** > **Installed Apps** on the menu bar.
     b. Click **Android** or **iOS** tab, and select the applications from the list of detected or installed 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 enable or disable the feature that allows users to uninstall the Mobile Device Agent. Additionally, you can select whether to allow users to configure Mobile Security device agent settings.

  The following is a list of features associated with uninstall protection:

  - turn On/Off uninstall protection from the administration console
  - password length must have a minimum of six (6) and a maximum of twelve (12) characters; password may contain numbers, characters or symbols.
  - password can be set for each group from the administration console.

  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 **Spam Prevention Policy**, **Call Filtering Policy** and **Web Threat Protection Policy** are not affected when this option is selected. For more information, see *Spam SMS Prevention Policies on page 5-14*, *Spam WAP Push Prevention Policies on page 5-16*, and *Security Policy on page 5-11*.

- **Update Settings**: You can select to have the Mobile Security Management Server notify Mobile Device Agents when a new

component is available for update. Or 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.

- **Log Settings**: When Mobile Device Agents detect a security risk, such as a malware on Android operating system, a log is generated on the mobile device.

Wi-Fi Policy

Wi-Fi Policy enables you to deliver your organization's Wi-Fi network information to Android and iOS mobile devices; including the network name, security type and password.

To configure Wi-Fi policy settings, click **Policies**, then click the policy name, and then click **Wi-Fi Policy**.

Exchange ActiveSync Policy

Exchange ActiveSync Policy enables you to create an Exchange ActiveSync policy for your organization and deliver it to iOS mobile devices.

To configure Exchange ActiveSync policy settings, click **Policies**, then click the policy name, and then click **Exchange ActiveSync Policy**.

VPN Policy

VPN policy settings enable you to create a VPN Policy for your organization and deliver it to iOS mobile devices.

To configure VPN policy settings, click **Policies**, then click the policy name, and then click **VPN Policy**

Global HTTP Proxy Policy

Global HTTP Proxy Policy enables you to deliver your organization's proxy information to mobile devices. This policy only applies to iOS mobile devices that are in supervised mode.

To configure global HTTP proxy policy settings, click **Policies**, then click the policy name, and then click **Global HTTP Proxy Policy**

Certificate Policy

Certificate Policy enables you to import certificates that you need to deploy on iOS mobile devices.

To configure certificate policy settings, click **Policies**, then click the policy name, and then click **Certificate Policy**.

Single Sign-On Policy

Single sign-on (SSO) policy enables the users to use the same credentials across applications, including Mobile Securityand applications from the App Store. Each new application configured with SSO certification verifies user permissions for enterprise resources, and logs users in without requiring them to reenter their passwords.

The single sign-on policy includes the following information:

- **Name**: the Kerberos principal name.
- **Realm**: The Kerberos realm name.

  The Kerberos ream name should be properly capitalized.
- **URL Prefixes** (Optional): List of URLs that must be matched in order to use an account for Kerberos authentication over HTTP. If this field is blank, the account is eligible to match all http and https URLs. The URL matching patterns must begin with either http or https.

  Each entry of this list must contain a URL prefix. Only the URLs that begin with one of the strings in an account are allowed to access the Kerberos ticket. URL matching patterns must include the scheme. For example, http://www.example.com/. If a matching pattern does not end in /, it will automatically add a / to the URL.
- **Application Identifiers** (Optional): List of application identifiers that are allowed to use the account. I f this field is blank, this account matches all application identifiers.

The **Application Identifiers** array must contain strings that match application bundle IDs. These strings may be exact matches (such as com.mycompany.myapp) or may specify a prefix match on the bundle ID by using the * wildcard character. The wildcard character must appear after a period character (.), and may appear only at the end of the string (such as com.mycompany.*). When a wildcard is used, any application whose bundle ID begins with the prefix is granted access to the account.

To configure Single Sign-On Policy for iOS settings, click **Policies**, then click the policy name, and then click **Single Sign-On Policy**.

AirPlay/AirPrint Policy

AirPlay/AirPrint policy settings enable you to create AirPlay and AirPrint policies for your organization and deliver it to iOS mobile devices.

To configure AirPlay and/or AirPrint policy settings, click **Policies**, then click the policy name, and then click **AirPlay/AirPrint Policy**.

Cellular Network Policy

Celluar network policy settings enables you to configure cellular network settings for your organization and deliver it to iOS mobile devices.

To configure the celluar network policy settings, click **Policies**, then click the policy name, and then click **Celluar Network Policy**.

Theme Policy

Theme policy settings enable you to push a font and set a wallpaper for home screen and lock screen for the iOS mobile devices. This policy applies to iOS mobile devices that are in the supervised mode only.

To configure theme policy settings, click **Policies**, then click the policy name, and then click **Theme Policy**.

Managed Domains Policy

Managed domains policy enables you to configure the email and/or web domains that your organization manages.

- Unmarked Email Domains: When a user is composing an email using the system email client, any email address entered which does not match the configured domains will be highlighted (marked) in red. Administrators should consider using this functionality, to warn users who may be inadvertently attempting to send sensitive information to untrusted email addresses.
- Managed Safari Web Domains: You can specify that files downloaded from specific domains using Safari may only be opened with managed apps. For example, a PDF downloaded from internal.example.com may be opened with Adobe Reader (a managed app) but not Dropbox (an unmanaged app). This provides improved containerization of Safari and wider the use as an enterprise browser.

Important

You must disable the following iOS features in the Feature Lock Policy. Otherwise, the managed Safari Web domains settings will not have any effect, since the downloaded files can be opened with other (unmanaged) apps:

- Open documents from managed apps in other apps (7.0 or above)
- Open documents from other apps in managed apps (7.0 or above)

To configure managed domain policy settings, click **Policies**, then click the policy name, and then click **Managed Domain Policy**.

Security Policy

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

The **Security Policy** screen also enables you to manage Web threat protection policy for Android mobile devices. It also enables Android mobile devices to send the Web threat protection log back to the server.

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 5-3. 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 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.	

Section	Item	Description	Supported Mobile Device OS
	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.	
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	

Section	Item	Description	Supported Mobile Device OS
		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/	

Spam Prevention Policy

The spam prevention policy in Mobile Security provides protection against spam WAP push and SMS text messages.

To configure spam prevention policy settings, click **Policies**, then click the policy name, and then click **Spam Prevention Policy**.

Spam SMS Prevention Policies

Note

This feature is no longer supported.

This feature provides you server-side control of SMS spam prevention policies. The following features are available when configuring the SMS Spam Prevention Policies:

- enable or disable spam SMS prevention for mobile device
- configure the mobile device to use a blocked list, approved list or disable the SMS anti-spam feature for mobile device.
- configure an approved list from the administration console
- configure a blocked list from the administration console

Refer to the following table for approved or blocked filtering list configuration details.

TABLE 5-4. Filtering list configuration for Spam SMS Prevention Policy

CENTRAL CONTROL	USER CONTROL	DESCRIPTION
Disabled	Enabled	The user can edit the approved/blocked list on the mobile device agent. Mobile Security allows or blocks the messages based on the following priority: 1. Approved List on Mobile Device Agent 2. Blocked List on Mobile Device Agent
Enabled	Disabled	The user is only allowed to edit the approve/blocked list on the mobile device agent. Mobile Security allows or blocks the messages based on the following priority: 1. Approved List or Blocked List on server 2. Approved List on Mobile Device Agent 3. Blocked List on Mobile Device Agent

Central Control	User Control	Description
Enabled	Enabled	The user can view or edit the approved/blocked list defined by the administrator and can also use the approved/blocked list on the mobile device agent. When the security policies sync with the mobile device agent, it does not sync the filtering lists, and updates all other settings according to the policies. Mobile Security allows or blocks the messages based on the following priority: 1. Approved List on Mobile Device Agent 2. Blocked List on Mobile Device Agent 3. Approved List or Blocked List on server

Note

The SMS approved and blocked list must use the format: "[name1:]number1; [name2:]number2;...".

The 'name' length should not exceed 30 characters, while phone number should be between 4 and 20 characters long and can contain the following: 0-9, +, -, #, (,) and spaces. The maximum number of entries should not exceed 200.

Spam WAP Push Prevention Policies

Note

This feature is no longer supported.

This feature provides you server-side control of WAP Push Prevention. If enabled, you can select whether to use a WAP approved list.

Note

The WAP approved list must use the format: "[name1:]number1; [name2:]number2;...".

The 'name' length should not exceed 30 characters, while phone number should be between 4 and 20 characters long and can contain the following: 0-9, +, -, #, (,) and spaces. The maximum number of entries should not exceed 200.

The following is a list of features available when configuring WAP Push Prevention policies:

- enable or disable WAP Push Prevention for mobile device
- configure the mobile device to use an approved list or disable WAP Push Prevention on the mobile device
- configure an approved list from the administration console
- if the administrator has enabled server-side control, the user will be unable to change the WAP Push Prevention type defined by the administrator
- if the administrator has disable server-side control, and allowed users to configure Mobile Security settings on mobile device, the user will be unable to view or edit the WAP Push Prevention list configured by the administrator, and may edit the personal WAP Push Prevention list on the mobile device side

Note

The users' personal settings for spam messages will be cleared after the Spam Prevention Policy is applied on the Mobile Device Agents.

Call Filtering Policy

Note

This feature is no longer supported.

This feature provides you server-side control of call filtering policies. To configure call filtering policy settings, click **Policies**, then click the policy name, and then click **Filtering Policy**.

The following features are available when configuring the Call Filtering Policies:

- enable or disable call filtering for mobile device
- configure the mobile device to use a blocked list or an approved list
- configure an approved list from the administration console
- configure a blocked list from the administration console

Refer to the following table for approved or blocked filtering list configuration details.

TABLE 5-5. Filtering list configuration for Call Filtering Policy

CENTRAL CONTROL	USER CONTROL	DESCRIPTION
Disabled	Enabled	The user can edit the approved/blocked list on the mobile device agent. Mobile Security allows or blocks the URLs based on the following priority: 1. Approved List on Mobile Device Agent 2. Blocked List on Mobile Device Agent

Central Control	User Control	Description
Enabled	Disabled	The user is only allowed to edit the approved/blocked list on the mobile device agent. Mobile Security allows or blocks the incoming calls based on the following priority: 1. Blocked List on server 2. Approved List on Mobile Device Agent 3. Blocked List on Mobile Device Agent You can also configure server-side control for outgoing calls on Android mobile devices.
Enabled	Enabled	The user can view or edit the approved/blocked list defined by the administrator and can also use the approved/blocked list on the mobile device agent. When the security policies sync with the mobile device agent, it does not sync the filtering lists, and updates all other settings according to the policies. Mobile Security allows or blocks the incoming calls based on the following priority: 1. Approved List on Mobile Device Agent 2. Blocked List on Mobile Device Agent 3. Blocked List on server You can also configure server-side control for outgoing calls on Android mobile devices.

Note

The call filtering approved and blocked list must use the format: "[name1:]number1;[name2:]number2;...".

The 'name' length should not exceed 30 characters, while phone number should be between 4 and 20 characters long and can contain the following: 0-9, +, -, #, (,) and spaces. The maximum number of entries should not exceed 200.

Password Policy

The password policy prevents unauthorized access to data on mobile devices.

To configure password policy settings, click **Policies**, then click the policy name, and then click **Password Policy** from the left-menu.

Feature Lock Policy

With this feature, you can restrict (disable) or allow (enable) the use of certain mobile device features/components. For example, you can disable the camera for all mobile devices in a particular group.

Note

The Tethering feature is no longer supported.

To configure Feature Lock Policy settings, click **Policies**, then click the policy name, and then click **Feature Lock Policy** from the left-menu.

See *Supported Mobile Device OS Features on page 1-18* for the list of supported features/components.

WARNING!

Use caution while disabling WLAN/WIFI and/or Microsoft ActiveSync. The mobile device may not be able to communicate with the server if both these options are unavailable.

For Android mobile devices, you can also add access point(s) to control the availability of the device components within the range of those access point(s).

Compliance Policy

Compliance policy enables you to set the compliance criteria for the mobile devices. If any mobile device does not match the criteria, Mobile Security displays its non-compliant status on the server UI. Mobile Security also sends an email to the non-compliant iOS mobile device, while it displays a notification on non-compliant Android mobile devices. The compliance check list includes:

- **Rooted/Jailbroken**—checks whether the mobile device is rooted/jailbroken or not.
- **Unencrypted**—checks whether the encryption is enabled on the mobile device or not
- **OS version check**—checks whether the OS version matches the defined criteria or not.

To configure compliance policy settings, click **Policies**, then click the policy name, and then click **Compliance Policy**.

Application Monitor and Control Policy

Application monitor and control policies provide you server-side control of the applications installed on mobile devices and push the required applications to the mobile devices.

To configure application monitor and control policy settings, click **Policies**, then click the policy name, and then click **Application Monitor and Control Policy**.

- **Required Applications**—using this option will push all the applications that you add in the list, to the mobile devices. You can also link a VPN to applications, so that the applications always use this VPN to connect to the network.
- **Permitted Applications**—control the applications installed on mobile devices by using approved and blocked lists.

For iOS mobile devices, Mobile Security sends notification to administrator and the user for any application that does not comply with the policy.

For Android mobile devices, Mobile Security blocks the application that does not comply with the policy and will allow all others.

- **Enable system apps blocking** (Android only):

  if selected, Mobile Security will block all the system apps on Android mobile devices.

- **Enable Application Category**: select the application category that you want to enable or disable on mobile devices. You can also make the exception by adding the applications that belong to these categories to the approved or blocked list. For example, if you have disabled a category type Games, Mobile Security will block all the applications that belong to this category, unless any such application exists in the approved list.

  Mobile Security allows or blocks the applications according to the following priority:

  1. **Approved List**—Mobile Security allows applications that are in the approved list even if they belong to the category that you have disabled.
  2. **Blocked List**—Mobile Security blocks applications that are in the blocked list even if they belong to the category that you have enabled.
  3. **Application permissions**—Mobile Security allows or blocks applications according to your selected permission status for the category that they belong to.

- **Enable Application Permissions** (for Android only): select the application services that you want to enable or disable on Android mobile devices. You can also make the exception by adding the applications that use these services to the approved or blocked list. For example, if you have disabled service type **Read Data**, Mobile Security will block all the applications that use the Read Data service, unless any such application exists in the approved list.

Mobile Security allows or blocks the applications according to the following priority:

1. **Approved List**—Mobile Security allows applications that are in the approved list even if they use the services that you have disabled.
2. **Blocked List**—Mobile Security blocks applications that are in the blocked list even if they use the services that you have enabled.
3. **Application permissions**—Mobile Security allows or blocks applications according to your selected permission status for the services that they use.

- **Only allow the following applications**: add the applications to the approved list that you want to allow users to use on their mobile devices. If enabled:
  - Mobile Security displays a pop-up warning message on Android mobile devices if it detects applications that are not in the approved list.
  - On iOS mobile devices, if Mobile Security detects any application that is not in the approved list, Mobile Security sends an email notification to the user.
- **Only block the following applications**: add the applications to the blocked list that you do not want users to use on their mobile devices. If enabled:
  - Mobile Security displays a pop-up warning message on Android mobile devices if it detects applications that are in the blocked list.
  - On iOS mobile devices, if Mobile Security detects any application that is in the blocked list, Mobile Security sends an email notification to the user.
- **Lock to App (for Supervised Mode Only)**—restrict the iOS mobile device to the specified application.

Mobile Security checks for restricted applications and sends email alert to the users:

- automatically according to the **Information Collection Frequency** settings in **Administration** > **Communication Server Settings** > **Common Settings (tab)**, or
- when you update the **Information Collection Frequency** settings in **Administration** > **Communication Server Settings** > **Common Settings (tab)**.

Volume Purchasing Program Policy

This policy enables the administrator to import the iOS applications to the Mobile Security administration web console that are purchased through the Apple's Volume Purchase Program. Mobile Security will push all the applications in the Volume Purchasing Program List to mobile devices in a group.

To configure Volume Purchasing Program policy:

1. Add applications to the Enterprise App Store. See *Adding an Application on page 6-2* for the procedure.
2. Click **Policies**, then click the policy name, and then click **Volume Purchasing Program Policy**.
3. Click **Import** and then select applications to import from the Enterprise App Store.
4. Click **Save** to push all the applications to the iOS mobile devices.

Container Policy

This policy enables you to manage Samsung KNOX container security settings. You can configure approved list or blocked list for accounts, apply restrictions, and configure browser, password, and application setttings.

Note

You must configure KNOX license in Mobile Security before enabling this policy. To configure the KNOX license, navigate to **Administration** > **Product License** on the administration web console.

- **Account Settings**: Specify accounts that can be added or restricted on Samsung KNOX containers by using approved and/or blocked lists.
- **Restriction Settings**: Disable camera or file sharing on Samsung KNOX containers.
- **Browser Settings**: Configure security settings for the native Android web browser on Samsung KNOX containers.
- **Password Settings**: Configure password security settings for Samsung KNOX container.
- **Application Settings**: Configure the following lists:
  - **Filter Applications List**: Configure approved list or blocked list to restrict applications installation on Samsung KNOX container.
  - **Required Applications**: Configure the required applications list to specify applications that must be installed on Samsung KNOX.
  - **Disable Applications**: Configure the disable applications list to disable certain applications on the mobile device. If the applications on this list are installed on the mobile device, they will not be removed, but the user will not be able to use these applications.

To configure container policy settings, click **Policies**, then click the policy name, and then click **Container Policy**.

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 5-27*.
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 5-27* 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**.

Configuring Application Availability

Mobile Security enables you to configure apps that you want to make available on iOS and Android mobile devices for a particular 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 the number of apps for the policy, under the **Available Apps** column.

   The **Available Apps** screen displays.

4. Click **iOS Applications** or **Android Applications** tab.

5. Do one of the following:
   - To enable or disable an app, click on the button under the **Permission** column for the app to toggle.
   - To enable or disable all apps, click **Enable All** or **Disable All**.
6. Toggle the availability of a application in the **Permission** column.

Chapter 6

Managing Applications

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 the Enterprise App Store on page 6-2*
- *About Installed Apps on page 6-10*

About the Enterprise App Store

The Enterprise App Store enables you to create a list of webclips and apps for the users to download and install on their Android or iOS mobile devices.

You can also upload iOS applications purchased through Apple's Volume Purchase Program to the Enterprise App Store on the Mobile Security administration web console.

Managing Enterprise Apps

Adding an Application

Procedure

1. On the Mobile Security administration web console, go to **Applications** > **Enterprise App Store**.

   The **Enterprise App Store** screen displays.

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

3. Click **Add**.

   The **Add Application** window displays.

4. You can now add an application to the list using one of the following options:

   - **Add from local computer**—select an installation file for Android or iOS mobile devices.
   - **Add a Webclip**—type the application's URL and the application's icon will appear on the home screen of user's mobile device, and the link will open in the default web browser on the mobile device.
   - (Android) **Add from external application store**—type the link to the application in an external app store. The application's icon will appear on the home screen of user's mobile device, and the link will open in the default web browser on the mobile device.
   - (iOS) **Add app link from iTunes Store**—type the name of the VPP application you want to search in the **Search keyword** field, and

select a country to search the application in its Apple app store, and then select the application you want to add from the search results. Once added, the VPP application is only available in the **App Store** on Mobile Security administration web console. To push the application to mobile devices, you will need to add the application to the **Volume Purchasing Program Policy**. See *Volume Purchasing Program Policy on page 5-24* for the procedure.

5. Click **Continue**.

   The **Edit Application** screen displays.

6. Configure the following:

   - **Application name**: type a name for the application.
   - **Application icon**: if the application icon does not appear, click Upload app icon to select and upload the application icon.
   - **Application ID**: if the application ID does not appear, type the application ID.
   - **VPP codes file**: For iOS VPP application, upload the Volume Purchase Code files that you have received from Apple.
   - **Category**: select a category for the application.

     Note

     You must select a category from the drop-down list. To add or delete a category, click the **Category** button.

   - **Description**: type the description for the application.
   - **Publish**: select one of the following:
     - **Do not publish**—to upload the application on the server, but keep hidden from the mobile devices.
     - **Publish as production version**—to upload the application on the server, and publish it for mobile devices to download.

- **Publish as beta version**—to upload the application on the server, and publish it as a beta version for mobile devices to download.

- **Screenshots**: select and upload application screenshots.

7. Click **Continue**.

   The application appears in the applications list.

Editing Application Information

Procedure

1. On the Mobile Security administration web console, go to **Applications** > **Enterprise App Store**.

   The **Enterprise App Store** screen displays.

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

3. Click the application name whose information you want to edit.

   The **Edit Application** window displays.

4. Modify the details on the screen.

5. Click **Continue**.

Deleting Applications from the App Store

Procedure

1. On the Mobile Security administration web console, go to **Applications** > **Enterprise App Store**.

   The **Enterprise App Store** screen displays.

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

3. Select the applications that you want to delete.

4. Click **Delete** and then click **OK** on the confirmation dialog box.

Managing Application Categories

Adding an Application Category

Procedure

1. On the Mobile Security administration web console, go to **Applications** > **Enterprise App Store**.

   The **Enterprise App Store** screen displays.

2. Click the **Android** or **iOS** tab.
3. Click **Manage Category**.
4. Click **Add**.

   The **Add Category** window displays.

5. Type the category name and description, and then click **Save**.

Editing an Application Category

Procedure

1. On the Mobile Security administration web console, go to **Applications** > **Enterprise App Store**.

   The **Enterprise App Store** screen displays.

2. Click the **iOS Applications** tab or **Android Applications** tab.
3. Click **Manage Category**.
4. Click the category name that you want to edit.

   The **Edit Category** window displays.

5. Modify the category details, and then click **Save**.

Deleting an Application Category

Procedure

1. On the Mobile Security administration web console, go to **Applications** > **Enterprise App Store**.

   The **Enterprise App Store** screen displays.

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

3. Click **Manage Category**.

4. Select the categories that you want to delete, click **Delete**, and then click **OK** on the confirmation dialog box.

Managing Apps Purchased through the Volume Purchase Program

Important

VPP is only available in certain regions. Make sure that your organization qualifies. Refer to the following link for the details:

http://www.apple.com/business/vpp/

Apple uses redemption codes and the Volume Purchase Program (VPP) licenses for the volume purchase of apps. Since you cannot convert the redemption codes into VPP licenses, Mobile Security supports both of these options.

The Volume Purchase Program enables you to distribute VPP licenses to users or devices for iOS applications.

You can manage VPP apps by monitoring the number of remaining licenses and by reclaiming licenses. Users can use VPP apps even if they have not installed the Mobile Security client application on their mobile devices.

Note

Mobile Security does not push VPP apps to mobile devices. Users need to download them manually to their mobile devices from the Apple App Store from the following location: **App Store** > **Update** > **Purchased**.

Setting Up Volume Purchase Program Licenses

Procedure

1. Navigate to the following URL:

   http://www.apple.com/business/vpp/

2. Sign in with your Apple account and download the service token file from the Apple Volume Purchase Program web portal.

3. On the Mobile Security administration web console, go to **Applications** > **Enterprise App Store** > **iOS**.

   The **iOS Enterprise App Store** screen displays.

4. Go to **Volume Purchase Program (VPP) Management** > **VPP Setting**.

5. Upload the token file you downlaoded from the Apple web portal in the field provided, and wait until the upload completes.

6. Click **Sync Now**.

Assigning or Reclaiming VPP Licenses

Mobile Security enables you to assign or reclaim application licenses purchased through the Volume Purchase Program to a user or device.

Important

Before assigning or reclaiming applications, make sure that the Volume Purchase Program Licences are ready.

For more information, see *Setting Up Volume Purchase Program Licenses on page 6-7*.

Procedure

1. On the Mobile Security administration web console, go to **Applications** > **Enterprise App Store** > **iOS** > **Volume Purchase Program (VPP) Management**.
2. Under the **Application List**, locate the application and then click **Assign/Reclaim**.

   The **Assign/Reclaim Licenses** screen appears.
3. To assign licenses, perform the following steps.
   - Assigning license to a device:
     a. On the **Devices** tab, select a device or multiple devices with an **Unassigned** status.
     b. Click **Assign**.

     Note

     Volume Purchasing Program has the following limitations when assigning apps to devices:

     - You can only assign VPP apps to devices running on iOS 9 or later.
     - App developers must opt in to device assignment.

   - Assigning license to a user:
     a. On the **Users** tab, select a user or multiple users with an **Unassigned** status.
     b. Click **Assign**.

Note

Mobile Security sends a notification to users after a VPP license is assigned.

To modify the user notification settings, go to **Notification & Reports** > **User Notifications** > **VPP User Notification**.

The licenses are assigned successfully.

4. To reclaim licenses, perform the following steps.
   - Reclaiming license from a device:
     a. On the **Devices** tab, select a device or multiple devices with an **Assigned** status.
     b. Click **Reclaim**.
   - Reclaiming license from a user:
     a. On the **Users** tab, select a user or multiple users with an **Assigned** status.
     b. Click **Reclaim**.

   The licenses are reclaimed successfully.

Checking Status for VPP Users

Procedure

1. On the Mobile Security administration web console, go to **Applications** > **Enterprise App Store** > **iOS**.

   The **iOS Enterprise App Store** screen displays.

2. Go to **Volume Purchase Program (VPP) Management** > **VPP User List**.

3. Under the **Status** column, check the user status.

   The **Status** column may display one of the following statuses:

- - : You have not yet assigned any application to this user.
- **Registered**: You have assigned at least one application to the user, but the user has not yet associated the Apple ID with the email address.
- **Associated**: You have assigned at least one application to the user and the user has already associated the Apple ID with the email address.
- **Retired**: You have reclaimed all the licences assigned to this user.

Reclaiming All Licenses from a User

Mobile Security enables you to reclaim all the licenses from a user.

Procedure

1. On the Mobile Security administration web console, go to **Applications** > **Enterprise App Store** > **iOS**.

   The **iOS Enterprise App Store** screen displays.

2. Click the **Volume Purchase Program (VPP) Management** > **VPP User List**.
3. Select the users from the list, and then click **Retire**.
4. Click **Close** on the **User List** screen.

About Installed Apps

The **Installed Apps** screen lists all apps installed on all managed Android and iOS 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 5-4* and *Removing Applications from Approved List on page 5-5* 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 6-1. Installed Apps Information

INFORMATION	DESCRIPTION	ANDROID	IOS
App name	Name of the app	●	●
Version	App version number	●	●
Number of installations	Number of devices installed with the app	●	●

Viewing Installed Applications

Procedure

1. On the Mobile Security web console, go to **Applications** > **Installed Applications**.

   The **Installed Applications** tab appears.

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

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.

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 7-5*
- *Viewing Malicious iOS Profiles on page 7-6*

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 5-4* and *Removing Applications from Approved List on page 5-5* 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 5-4 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

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 8-2*
- *Viewing Mobile Device Agent Logs on page 8-2*
- *Log Maintenance on page 8-5*

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, policy violation 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.

Note

You can view SMS anti-spam, WAP push protection, and call filtering logs on the mobile devices.

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.
- Policy Violation Logs—these logs include information about the policy compliant status of Mobile Device Agents.
- 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.

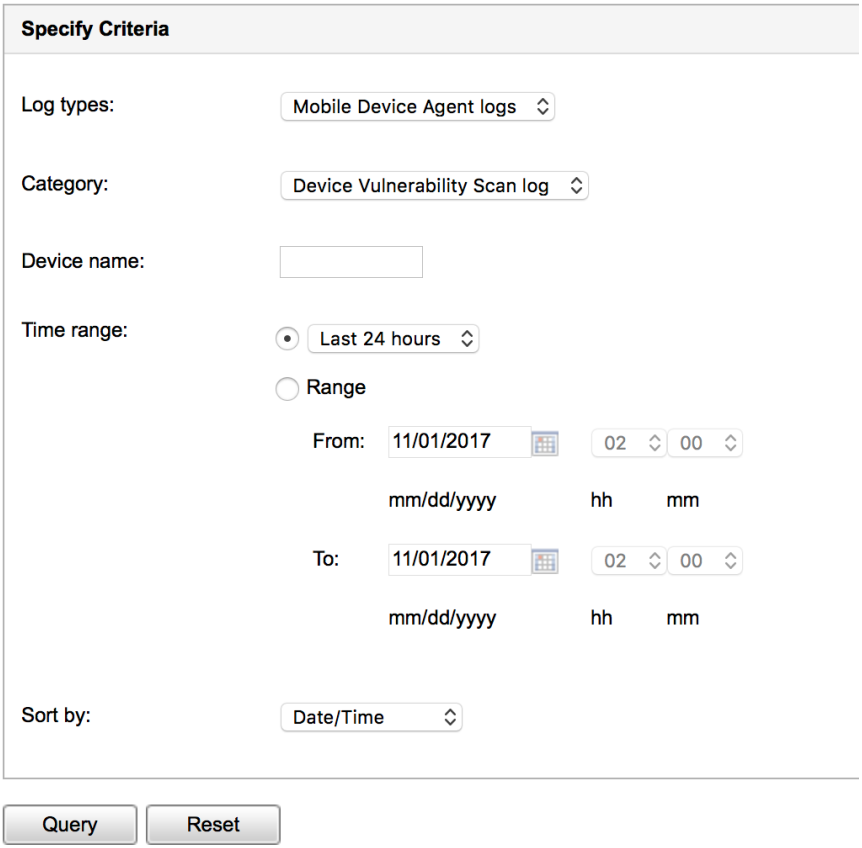

FIGURE 8-1. Log Query screen

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 9

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 9-2*
- *Configuring Notification Settings on page 9-2*
- *Configuring Email Notifications on page 9-2*
- *Administrator Notifications on page 9-7*
- *Reports on page 9-9*
- *User Notifications on page 9-14*

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**.

Configuring SMS Sender Settings

The Management Server controls and monitors SMS Senders connected to the server. The SMS Senders send messages to mobile devices to perform Mobile Device Agent installation, registration, component update, security policy setting, and remote wipe/lock/locate.

Use the SMS Sender Settings to:

- configure SMS sender phone numbers
- view SMS sender connection status
- set Mobile Device Agent installation message
- configure SMS sender disconnect notification

SMS Sender List

You need to configure SMS sender device phone numbers before the Management Server can instruct SMS senders to send messages to mobile devices.

Note

If you do not configure the phone number of an SMS sender in the SMS sender list, the Management Server prevents the SMS sender from sending messages to mobile devices.

Procedure

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

   The **Notifications/Reports Settings** screen displays. In **SMS Sender Settings** section, the list of SMS sender phone numbers and the connection status are displayed. If the SMS sender is connected to the Management Server successfully, the **Status** field displays: **Connected**.

   Note

   After three (3) failed attempts to send an SMS message(s), the mobile device will display "disconnected".

Configuring SMS Sender List

Specify the phone number of an SMS sender to enable the Mobile Security server to manage the SMS senders. SMS senders send messages to notify mobile devices to:

- download and install Mobile Device Agent
- register to the Mobile Security Management Module
- unregister from the Mobile Security Management Module
- update Mobile Device Agent components
- synchronize security policy settings with the Mobile Security Management Module
- remote wipe the mobile device
- remote lock the mobile device
- remote locate the mobile device

Procedure

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

   The **Notifications/Reports Settings** screen displays.
3. In **SMS Sender Settings** section, click **Add**, type the phone number of an SMS sender and click **Save**. The SMS sender appears in the list.
4. Check that the **Status** field displays "**Connected**" for the number you have configured. If the **Status** field displays "**Disconnected**", make sure the SMS sender device is connected to the Management Server.

   Note

   Existing SMS senders can be modified by clicking the phone number.

Monitoring SMS Senders

Mobile Security can monitor the status of SMS Senders and send out email notifications if any of the SMS Senders is disconnected for more than ten minutes. Additionally, the SMS Sender device also displays the connection status: Agent stopped, Agent running, Agent not in use, or Agent disconnected. See *Administrator Notifications on page 9-7* for the configuration details.

Editing an SMS Sender

Procedure

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

   The **Notifications/Reports Settings** screen displays.
3. In **SMS Sender Settings** section, click the phone number that you want to edit.

   A dialog box displays.
4. Edit the phone number in the field provided, and then click **Save**.
5. Click **Save** to save settings.

Deleting an SMS Sender

Procedure

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

   The **Notifications/Reports Settings** screen displays.
3. In **SMS Sender Settings** section, select the SMS Sender you want to delete, and click **Delete**.

4. Click **Save** to save settings.

Handling SMS Sender Client App

Setting up SMS Sender Client App

Procedure

1. Open the SMS Sender app on the Android mobile device.
2. Tap **Settings**, and then tap the following to configure:
   - **Server Address**: type the Management Server name or IP address and tap **OK**.
   - **Server Port**: type the administration Web console port number and tap **OK**.
   - **Phone Number**: type the phone number for the SMS Sender.
   - **Protocol Type**: select HTTP or HTTPS protocol for sending messages.
3. Tap **Start** to start the SMS Sender.

Stopping SMS Sender

Procedure

1. Open the SMS Sender app on the Android mobile device.
2. Tap **Stop** to stop the SMS Sender.

SMS Sender Status

Mobile Security updates the status of the SMS Sender on the mobile device. Depending on the connection status, the following status will appear on the device:

- Normal: SMS Sender is connected to the Management Server
- Stopped: SMS Sender is currently stopped.
- Not in use: the settings on the SMS Sender app does not match with the settings on the Mobile Security server.

Viewing SMS Sender History

Procedure

1. Open the SMS Sender app on the Android mobile device.
2. Tap **History** to view the messages that are sent to mobile devices.

Viewing SMS Sender Running Logs

Procedure

1. Start the SMS Sender app on the Android mobile device.
2. Tap **Running Logs** to view the SMS Sender running event logs.

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.

- **Deactivated Device Administrator for Mobile Security**—sends email notification to administrator when Mobile Security is disabled in the **Device administrators** list on any Android mobile device. Token variable `<%DEVICE%>` will be replaced by the mobile device name in the email.
- **APNS Certificate Expired Warning**—sends email notification to administrator one month before the APNs certificate expires.
- **VPP Token Expiry Warning**—sends email notification to administrator 15 days before the VPP token expires.
- **DEP Token Expiry Warning**—sends email notification to administrator 15 days before the DEP token 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 .

Important

Include the token variables provided in the default email template when modifying a notification message.

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.
- **Compliance Violation Report**—displays information on compliance violation.
- **Application Inventory Report**—displays information on top applications installed on Android and iOS devices.
- **Devices Enrollment Report**—displays information on device enrollment.
- **Devices Unenrollment Report**—displays information on device unenrollment.

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

TABLE 9-1. Report Tasks

TASK	DESCRIPTION
Generate	You can generate new reports whenever you need them. For more information, see *Generating Reports on page 9-10*.
View	You can view the last generated reports from the On-Demand tab. For more information, see *Viewing Reports on page 9-11*.
Send	You can choose to send reports via email whenever needed. For more information, see *Sending Reports on page 9-12*.
Schedule	You can specify a fixed schedule for sending reports to administrators and other users. For more information, see *Scheduling Reports on page 9-12*.

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 9-10*.

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 9-10*.

   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.
- **Policy Violation**—sends email notification to mobile devices if the compliance criteria is not met. Token variables `<%DEVICE%>` and `<%VIOLATION%>` will be replaced by the mobile device's name in the email, and the policies that it violates.
- **VPP User Notification**—sends email notification to a mobile device when administrator assigns a VPP app to a user.

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 10

Updating Components

This chapter shows you how to update Mobile Security components.

The chapter includes the following sections:

- *About Component Updates on page 10-2*
- *Updating Mobile Security Components on page 10-2*
- *Manually Updating a local AU server on page 10-5*

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 10-4* 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 10-2* 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 10-4* 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 10-2* or for scheduled update see *Scheduled Update on page 10-3*.
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 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, 8-2

C

call filtering
  filtering list configuration, 5-18
  filtering list format, 5-20
clearing corporate data on mobile devices, 3-14
command statuses, 2-19
Compatibility View, 2-4
compliance policy
  check list, 5-21
component updates
  about, 10-2
  download sources, 10-4
  local AU server, 10-5
  scheduled, 10-3

D

Dashboard
  application control status, 2-8
  encryption status, 2-8
  jailbreak/root status, 2-8
  mobile device status, 2-6
  patch and component update status, 2-7
  server update status, 2-7
device detection logs
  log types, 8-2
documentation feedback, 11-5

E

enterprise app store
  about, 6-2
Exchange ActiveSync Devices tab, 3-19
Exchange Connector
  configure, 2-21
Exchange Server
  data cleanup, 2-22
  integration settings, 2-21
  transfer, 2-22

F

Full license version, 2-4

G

General Policy
  log settings, 5-8
  uninstall protection features, 5-7
  update settings, 5-7

I

installed apps, 6-10
invitation statuses, 4-5

L

locking a mobile device, 3-13

M

Managed Devices tab, 3-2
MDA logs
  about, 8-2

Application Scan Logs, 8-2
Device Vulnerability Logs, 8-2
log types, 8-2
Network Protection Logs, 8-3
Policy Violation Logs, 8-2
query criteria, 8-4
Web Threat Protection Logs, 8-3
mobile device authentication, 1-17
Mobile Security
about, 1-2
Active Directory, 1-5
architecture, 1-3
Basic Security Model, 1-3
certificate
APNs certificate, 1-6
authority, 1-5
management, 2-20
public and private keys, 1-5
SCEP, 1-6
security credentials, 1-5
SSL certificate, 1-6
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
Exchange Connector, 1-5
Local Communication Server, 1-4
Management Server, 1-4
Microsoft SQL Server, 1-5
Mobile Device Agent, 1-5
OfficeScan, 1-2
SMS Sender, 1-4
SMTP server, 1-6
sub-groups, 3-2
unwanted network communications, 1-2
mobile threats, 1-2
spam messages, 1-2

N

notifications, 9-7
notifications and reports
about, 9-2
email message configuration, 9-14
SMS Agent Status, 9-6
SMS Sender, 9-2
token variables, 9-14

P

password
reset password, 3-15

R

regular updates, 1-17
reports, 9-9
root account properties, 2-12

S

security scanning, 1-16
send email alert, 5-24
spam
SMS, 5-15

filtering list configuration, 5-15
filtering list format, 5-16
WAP Push, 5-16
approved list format, 5-17
Super Administrator role properties, 2-13
support
resolve issues faster, 11-3

U

updating device information, 3-11
user account details, 2-15

W

Web security, 1-17
what's new
v9.6, 1-15
v9.6 SP1, 1-14
v9.7, 1-13
v9.7 Patch 2, 1-13
v9.7 Patch 3, 1-12
v9.8, 1-11
v9.8 sp1, 1-11
v9.8 sp2, 1-11
v9.8 sp2 Patch 1, 1-10
v9.8 sp3, 1-10
v9.8 sp4, 1-10
v9.8 sp5, 1-9
v9.8 sp5 critical patch 1, 1-9
v9.8 sp5 critical patch 2, 1-8
v9.8 sp5 critical patch 3, 1-8
v9.8 sp5 critical patch 4, 1-8
v9.8 sp5 critical patch 5, 1-7

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: TSEM909723/230410