TREND MICRO™

9.0

TREND MICRO™ Mobile Security™

Administrator's Guide

Comprehensive security for enterprise handhelds

Endpoint Security

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

http://docs.trendmicro.com

Document Part No. TSEM95922_130402

Release Date: July 2013

The user documentation for Trend Micro™ Mobile Security 9.0 for Enterprise 9.0 introduces the main features of the product and provides installation instructions for your production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product is available in the Online Help and the Knowledge Base at the Trend Micro website.

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.

Please evaluate this documentation on the following site:

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

Table of Contents

Preface

Chapter 1: Introduction

Chapter 2: Getting Started with Mobile Security

Chapter 3: Managing Mobile Devices

Chapter 4: Protecting Devices with Policies

Chapter 5: Managing Enterprise App Store

Chapter 6: Updating Components

Chapter 7: Viewing and Maintaining Logs

Chapter 8: Using Notifications and Reports

Chapter 9: Troubleshooting and Contacting Technical Support

Index

Preface

Preface

Welcome to the Trend Micro™ Mobile Security for Enterprise version 9.0 Administrator's Guide. This guide provides detailed information about all Mobile Security configuration options. Topics include how to update your software to keep protection current against the latest security risks, how to configure and use policies to support your security objectives, configuring scanning, synchronizing policies on mobile devices, and using logs and reports.

This preface discusses the following topics:

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

Audience

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

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

- Installing and configuring Windows servers
- Installing software on Windows servers
- Configuring and managing mobile devices (such as smartphones and Pocket PC/ Pocket PC Phone)
- 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
Tip	Recommendations or suggestions

Convention	Description
❗ 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 v9.0 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

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.

In addition to threats posed by malware, spam and other undesirable content, mobile devices are susceptible to hacking and Denial of Service (DoS) attacks. Mobile devices, many of which now have the same network connectivity traditionally associated only with larger computing devices like notebook computers and desktops, are now targets for these attacks.

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

About Trend Micro Mobile Security v9.0

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 firewall and 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.

Additionally, Mobile Security comes with a universal Encryption Module that provides logon password protection and data encryption features for Symbian and Windows Mobile devices. This Encryption Module helps prevent data from being compromised if a mobile device is lost or stolen.

WARNING!

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

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 Servers: • Local Communication Server (LCS)—this is a Communication Server deployed locally in your network. • Cloud Communication Server (CCS)—this is a Communication Server deployed in the cloud and you will not need to install this server. Trend Micro manages the Cloud Communication Server and you only need to connect to it from the Management Server. See *Comparison Between Local and Cloud Communication Servers on page 1-6*.	Required
SMS Senders	You can use SMS Sender to send SMS text messages to the users.	Optional
Exchange Connector	Trend Micro Mobile Security uses Exchange Connector to communicate with the Microsoft Exchange server, and detects the devices that use Exchange ActiveSync service.	Optional
Mobile Device Agent (MDA)	The Mobile Device Agent is installed on the managed mobile devices. The agent communicates with the Mobile Security server and executes the commands and policy settings on the mobile device.	Required

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
Microsoft SQL Server	The Microsoft SQL Server hosts the databases for Mobile Security server.	Required
Active Directory	The Mobile Security 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
SCEP	The Simple Certificate Enrollment Protocol (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	The Mobile Security server communicates through the Apple Push Notification Service (APNs) to iOS devices.	Required if you want to manage iOS mobile devices
SSL certificate	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 5 and above mobile devices
BES User Administration Tool	BES User Administration Tool is required to support manage BlackBerry devices that registered in BES server.	Required if you want to manage BlackBerry mobile devices
SMTP Server	Connect SMTP server to make sure administrators can get reports from Mobile Security 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	Not supported	Supported
Manage Symbian mobile devices	Not supported	Supported
Manage Windows Mobile devices	Not supported	Supported

What's New in This Release (v9.0)

The following table describes additional features that come with Trend Micro™ Mobile Security for Enterprise v9.0.

FEATURE NAME	DESCRIPTION
Standalone Management Server	This release of Trend Micro Mobile Security is independent of OfficeScan and can be installed directly on a Windows computer.

Feature Name	Description
Optional Cloud Communication Server	In addition to the Communication Server installed locally (Local Communication Server), this release also provides the option to use the Communication Server deployed in the Cloud (Cloud Communication Server). The administrators do not need to install the Cloud Communication Server, and it is maintained by Trend Micro.
Exchange Server Integration	Provides integration with the Microsoft Exchange Server, and supports iOS, Android and Windows Phone mobile devices that use Exchange ActiveSync service.
Template-based Policies	Enables you to create, copy or delete security policies and assign it to a certain mobile device group.
Support for Multiple Administrator Accounts	Enables you to create multiple administrator accounts with different roles that can be customized as and when required.
Updated Device Statuses	Displays more appropriate current status for mobile devices with the updated device status list.
iOS Device Provisioning	Enables you to push the required corporate certificates to the iOS mobile devices.
Supervised Device Management for iOS Mobile Devices	This release also adds the support for supervised iOS mobile devices.
Dashboard Screen Management	Enables you to manage the information displayed on the **Dashboard** screen in the form of widgets. You can add or remove the widgets according to your needs.
Server Command Confirmation	Provides the **Command Queue Management** interface that displays the current status of every command executed from the server.
Application Control Using Categories	Enables you to allow or block the installation of applications belonging to the certain categories on iOS and Android mobile devices using approved and blocked lists.
Mobile Device Enrollment Using QR-code	Introduces mobile device enrollment using QR-code that is sent in the user's email.

FEATURE NAME	DESCRIPTION
Feature Lock Policy Enhancement	Adds more features and OS components to the feature lock list for the administrator to control their availability on mobile devices.
iOS Volume Purchase Program Support	Enables you to import the iOS applications to the Mobile Security administration Web console that are purchased through the Apple's Volume Purchase Program.
Updated Mobile Device Agent Interface	Introduces the new user interface for Android and iOS mobile device agents.
Integration with MARS	Provides server and Android mobile device agent integration with Trend Micro Mobile Application Reputation Service (MARS) for applications security risk and resource usage.
Administrator Reports Download	Enables you to download the Administrator Reports from the Mobile Security administration Web console.
Policy Violation Log	Provides Policy Violation Log for Android mobile devices.
Integration with Trend Micro Control Manager	Trend Micro Mobile Security provides integration with Trend Micro Control Manager. This integration enables Control Manager administrators to deliver corporate policies to the mobile devices and allows them to view the Mobile Security **Dashboard** screen in Control Manager.

What's New in Release 8.0 SP1

The following table describes additional features that were introduced in Trend Micro™ Mobile Security for Enterprise v8.0 Service Pack 1 (SP1).

FEATURE NAME	DESCRIPTION
Authentication Based on Device Identity	Enables you to authenticate a batch of mobile devices using their IMEI numbers and/or Wi-Fi MAC addresses.
Unmanaged Group for Android and iOS	Introduces a group "Unmanaged" for Android mobile devices on which 'Device administrator' is deactivated, and for iOS mobile devices on which the enrollment profiles are removed.

Feature Name	Description
Enhanced Event Logs	Provides enhanced event logs to record events related to mobile device password reset, remote locate, remote lock and remote wipe.
Customizable Enrollment URL	Provides a shorter and customizable URL for the enrollment of mobile devices.
Simple iOS client	Introduces an iOS client for easy user authentication and enrollment using user email address. The iOS client also provides access to the Enterprise App Store on the mobile device.

What's New in Release 8.0

The following table describes additional features that were introduced in Trend Micro™ Mobile Security for Enterprise v8.0.

Feature Name	Description
Agent Customization	Enables you to preset the server IP address and port number into the Android installation package.
Web Proxy Support for Android	Enables you to set Web proxy in Android mobile devices.
HTTP(S) Push Notification Setting for Android	Provides setting to enable or disable the HTTP(S) push notifications for Android mobile devices.
Simpler Provisioning	Enables you to configure server IP address, domain name and server port number in Android mobile devices in advance, to reduce the effort of deployment and enrollment of mobile devices.
Scan After Pattern Update	Automatically starts scanning the mobile device for security threats after successful pattern update, and displays the progress in the notification bar.

Feature Name	Description
Web Threat Protection Policy	Enables you to manage Web threat protection policy from the Mobile Security server and deploys it on Android mobile devices. It also enables Android mobile devices to send the Web threat protection log back to the server.
Adds SD Card Restriction for Android	Enables you to control the availability of the SD card for Android mobile devices.
Application Inventory	Maintains the list of installed applications on mobile devices and displays it on the device status screen.
Application Control	Enables you to allow or block the installation of certain applications on mobile devices using approved and blocked lists.
Application Push	Enables you to push the application installation package or Web link of the application to mobile devices for installation.
Selective Wipe	Enables you to delete all the corporate data from the server, without deleting the user’s personal data.
Compliance Check	Enables you to set the compliance criteria on the server, and checks the mobile devices for compliance.
Optional Authentication using Active Directory	Enables you to set user authentication using Active Directory (AD) or Mobile Security database for Symbian, Windows Mobile, iOS and Android mobile devices for registration.
Dashboard Screen	Introduces the **Dashboard** screen to replace the old **Summary** screen on the Web console to provide the status summary of server components and mobile devices.
Scheduled Reports	Enables you to configure Mobile Security to send scheduled reports at the pre-defined intervals.
Quick Configuration Verification Screen	Introduces the **Mobile Security Configuration and Verification** screen that enables you to quickly verify Mobile Security configuration and identifies the problems, if any. If the configuration verification screen detects any wrong configuration setting, it provides suggestions to correct it.

Feature Name	Description
On-Demand Remote Password Reset for iOS and Android	Enables you to reset the password remotely for iOS and Android mobile devices from the Web console.
Enterprise App Store	Enables you to create a list of webclips and apps for the users to download and install on their mobile devices.

What's New in Release 7.1

The following table describes additional features that were introduced in Trend Micro™ Mobile Security for Enterprise v7.1.

Feature Name	Description
Support for iOS and Blackberry Mobile Devices	Mobile Security v7.1 added support for iOS and Blackberry mobile devices.
Integrated with Active Directory	Mobile Security v7.1 leverages the corporate's Active Directory (AD) for importing users and for performing user authentication.
Updated Architecture	In Mobile Security v7.1, single and dual server deployment models are introduced. SMS Gateway is also removed in v7.1.
Provisioning Policy	This version introduces the provisioning policy for mobile devices.

What's New in the Release 7.0

This section describes additional features that were introduced in Trend Micro™ Mobile Security for Enterprise v7.0.

Feature Name	Description
Support for Android Mobile Devices	Mobile Security v7.0 added support for Android v2.1 or above mobile devices.
Call Filtering Policies	Enables the administrator to control the incoming or outgoing calls on Android mobile devices.
Updated Feature Locking	Enables the administrator to control the availability of certain components for Android mobile devices that are within the range of certain access point(s).
Locate Remote Device	Enables the administrator to locate the remote device through the wireless network or by using mobile device's GPS and displaying its location on Google Maps. This new feature helps locate the lost, stolen or misplaced mobile devices.
Updated Architecture	In Mobile Security v7.0, SMS Gateway is added as an alternate to SMS Sender to send SMS messages to mobile devices.

Main Mobile Device Agent Features

Feature Name	Description
Anti-Malware 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 and enables you to quarantine and delete infected files.
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 Web sites and the Web sites 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 Web sites that were blocked by Web Reputation or Parental Controls in their specific logs.

FEATURE NAME	DESCRIPTION
SMS Anti-Spam	Mobile devices often receive unwanted messages or spam through SMS messaging. To filter unwanted SMS messages into a spam folder, you can specify the phone numbers from which all SMS messages will be considered spam or you can specify a list of approved phone numbers and configure Mobile Security to filter all messages from senders that are not in the approved list. You can also filter unidentified SMS messages or messages without sender numbers. Your mobile device will automatically store these messages to the spam folder in your inbox. **Note** The SMS Anti-Spam feature is not available on mobile devices without phone capabilities.
Call Filtering	Mobile Security enables you to filter incoming or outgoing calls from the server. You can configure Mobile Security to block incoming calls from certain phone numbers or you can specify a list of approved phone numbers to which the calls may be made from the mobile device. Mobile Security also enables mobile device users to specify their own Blocked or Approved list to filter unwanted incoming calls. **Note** The Call Filtering feature is not available on mobile devices without phone capabilities.

Feature Name	Description
WAP-Push Protection	WAP-Push is a powerful method of delivering content to mobile devices automatically. To initiate the delivery of content, special messages called WAP-Push messages are sent to users. These messages typically contain information about the content and serve as a method by which users can accept or refuse the content. Malicious users have been known to send out inaccurate or uninformative WAP-Push messages to trick users into accepting content that can include unwanted applications, system settings, and even malware. Mobile Security lets you use a list of trusted senders to filter WAP-Push messages and prevent unwanted content from reaching mobile devices. The WAP-Push protection feature is not available on mobile devices without phone capabilities.
Authentication	After installing the Mobile Device Agent a mobile device is associated with a user. The user must type a password (also known as the power-on password) to log on to the mobile device.
Data Encryption	Mobile Security provides dynamic data encryption for data stored on mobile devices and memory cards. You can specify the type of data to be encrypted and the encryption algorithm to use.
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.
Firewall (BlackBerry, Symbian and Windows Mobile only)	Mobile Security includes the Trend Micro firewall module, which comes with predefined security levels to filter network traffic. You can also define your own filtering rules and filter network traffic from specific IP addresses and on specific ports. The Intrusion Detection System (IDS) enables you to prevent attempts to continually send multiple packets to mobile devices. Such attempts typically constitute a Denial of Service (DoS) attack and can render your mobile device too busy to accept other connections.

FEATURE NAME	DESCRIPTION
Logs	The following Mobile Device Agent logs are available on the Management Server: • malware protection log • Web threat protection log • encryption log • firewall log • event log • violation log You can view the following logs on mobile devices: • Windows Mobile and Symbian: • virus/malware logs • firewall logs • SMS anti-spam logs • WAP Push protection logs • task logs • Android: • malware scan history • 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 per platform.

TABLE 1-3. Trend Micro Mobile Security 9.0 Feature Matrix

POLICY	FEATURES	SETTINGS					
Provisioning	Wi-Fi	Wi-Fi configuration	●	●	●		
	Exchange ActiveSync	Exchange ActiveSync configuration	●				
	VPN	VPN configuration	●		●		
	Global HTTP Proxy	Global HTTP Proxy configuration	●				
	Certificate	Certificate configuration	●				
Device Security	Malware Protection	Real-time scan		●		●	●
		Card scan				●	●
		Scan after pattern update		●			

Policy	Features	Settings	🍎	🤖	⁙	⊞	S
Data Protection	Spam SMS Prevention	Server-side control		●	●	●	●
		Use blocked list		●	●	●	●
		Use approved list		●	●	●	●
	Spam WAP Push Prevention	Server-side control		●		●	●
		Use approved list		●		●	●
	Call Filtering	Server-side control		●	●		
		Use blocked list		●	●		
		Use approved list		●	●		
	Firewall	Enable firewall			●	●	●
		Enable Intrusion Detection System (IDS)				●	●
	Web Threat Protection	Server-side control		●			
		Use blocked list		●			
		Use approved list		●			

Policy	Features	Settings					
Data Protection	Password Settings	Use Password for login	●	●	●	●	
		Admin password				●	
		Allow simple password	●	●	●	●	
		Require alphanumeric password	●	●	●	●	
		Minimum password length	●	●	●	●	
		Password expiration	●	●		●	
		Password history	●	●		●	
		Auto-lock	●	●		●	
		Password failure action	●	●	●	●	
	Encryption	Encrypt PIM				●	
		Encrypt documents				●	
		Encrypt memory cards				●	
	Feature Lock	Camera	●	●		●	
		FaceTime	●				
		Screen capture	●				
		Apps installation	●				

POLICY	FEATURES	SETTINGS					
Data Protection	Feature Lock	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	●				
		Bluetooth and Bluetooth discovery		●		●	
		Infrared				●	
		USB storage				●	
		WLAN/Wi-Fi		●		●	
		3G data network		●			

Policy	Features	Settings		🤖	⁘	⊞	S
Data Protection	Feature Lock	Tethering		●			
		Developer mode		●			
		Serial				●	
		Speaker/speakerphone/ microphone			●	●	
		Microsoft ActiveSync				●	
		MMS/SMS				●	
		Restrict memory cards		●		●	
		Restrict GPS				●	
		Siri	●				
		Siri while device is locked	●				
		Enable profnity filter	●				
		Enable access to iCloud services	●				
		Cloud backup	●				
		Cloud document sync	●				
		Photo Stream	●				

Policy	Features	Settings		🤖	⁘	⊞	S
Data Protection	Feature Lock	Shared Photo Streams	●				
		Diagnostic data	●				
		Accept untrusted Transport Layer Security (TLS)	●				
		Force iTunes to store password	●				
		YouTube	●				
		iTunes	●				
		Safari Web browser	●				
		AutoFill	●				
		JavaScript	●				
		Popups	●				
		Force fraud warning	●				
		Accept cookies	●				
		Removing apps (Supervised only)	●				
		Bookstore (Supervised only)	●				

Policy	Features	Settings					
Data Protection	Feature Lock	Erotica (Supervised only)	●				
		Configuration Profile Installation (Supervised only)	●				
		iMessage (Supervised only)	●				
		Ratings region	●				
		Movies	●				
		TV Shows	●				
		Apps	●				
Remote control		Register	●	●	●	●	●
		Update	●	●	●	●	●
	Anti-theft	Remote locate		●	●		
		Remote lock	●	●	●	●	
		Remote wipe	●	●	●	●	
		Reset password	●	●	●	●	

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:

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

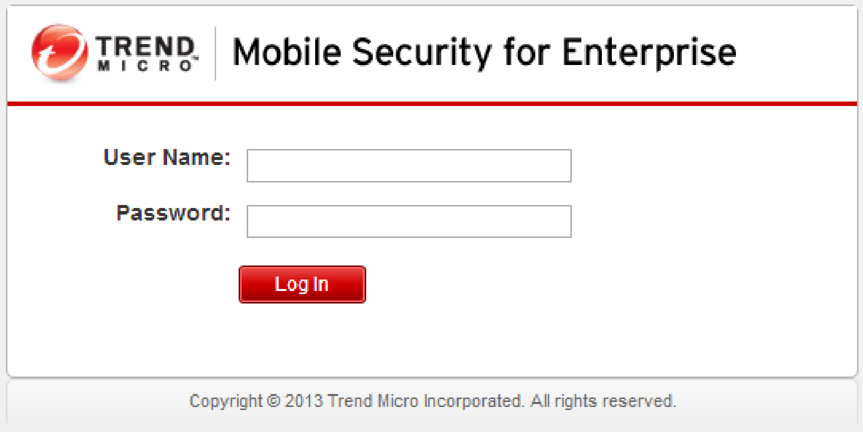
1. Log on to the administration Web console using the following URL structure:

```
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.



Mobile Security for Enterprise

User Name:

Password:

Copyright © 2013 Trend Micro Incorporated. All rights reserved.

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 on page 2-15* for the procedure.

Important

If you are using Internet Explorer to access the administration Web console, make sure the following:

- the **Compatibility View for Web sites** 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 Web site, 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 Web site 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 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 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 the device health status and device's operating system summary.
- **Health**—shows the 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 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 server, but does not comply with the server policies.
        - **Out of Sync**—shows that the device is enrolled to the Mobile Security 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 server.
    - View the total number of enrolled and unregistered mobile devices managed by Mobile Security.

      A mobile device may remain unregistered if one of the following happens:

        - a connection to the Communication Server is unsuccessful
        - the mobile device user has deleted the registration SMS message
    - 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 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 server modules
        - **Last Updated**—the time and date of the last update
- **Inventory**—shows mobile device operating system version summary, telephone carriers summary, mobile device vendors summary and top 10 applications installed on mobile devices.

- **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
- **Protection**—shows the lists of top five (5) security threats and top five (5) blocked Web sites.

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 Device Authentication

Trend Micro Mobile Security enables you to configure device authentication based on the Active Directory (AD) or the Mobile Security database. You can also allow mobile devices to enroll with the Mobile Security server without authentication. 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.

Managing Administrator Accounts

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

Default Administrator User Name and Role

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

TABLE 2-1. The root account properties

ROOT ACCOUNT PROPERTIES		CAN BE MODIFIED?
Admin Accounts	User name	No
	Full name	Yes
	Password	Yes
	Email address	Yes
	Mobile phone number	Yes
Admin Roles	Admin 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 Admin Role on page 2-17* for the detailed procedure.

TABLE 2-2. The Super Administrator role properties

SUPER ADMINISTRATOR ROLE PROPERTIES		CAN BE MODIFIED?
User Details	Admin 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
	Exchange Server Integration	Supported	Not supported
	Configuration and Verification	Supported	Not supported
	Product License	Supported	Not supported

Server Components	Permissions	Super Administrator	Group Administrator
Notification/ Reports	Log Query	All the groups	Managed groups only
	Log Maintenance	All the groups	Managed groups only
	Administrator Notification/Reports	Supported	Not supported
	User Notification	Supported	Not supported
	Settings	Supported	Not supported
App Store	App Store	Supported	Not supported
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

Server Components	Permissions	Super Administrator	Group Administrator
Devices	View devices	Supported	Supported for managed groups only
	Add group	Supported	Supported
	Invite Devices	Supported	Supported for managed groups only
	Exchange ActiveSync Devices	Supported	Supported for managed groups only

Adding Administrator Accounts

Procedure

1. Log on to the Mobile Security administration Web console.
2. Click **Administration** > **Administrator Account Management**.
3. On the **Admin Accounts** tab, click **Create** to add a new account.

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

5. Under section **Admin Role**, select the role from the **Choose the admin role:** drop-down list.

   See *Creating an Admin Role on page 2-16* for the procedure for creating admin roles

6. Click **Save**.

Editing an Administrator Account

Procedure

1. Log on to the Mobile Security administration Web console.
2. Click **Administration** > **Administrator Account Management**.
3. On the **Admin Accounts** tab, click **Create** to add a new account.

   The **Edit Admin Account** screen appears.

4. Modify the user account details and access role as required.

   - User Details

     - **User 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**.

- **Admin Role**

  - **Choose the admin role**: select the admin role from the drop-down list.

    For the procedure to create an admin role, see *Creating an Admin Role on page 2-16*.

5. Click **Save**.

Deleting an Administrator Account

Procedure

1. Log on to the Mobile Security administration Web console.
2. Click **Administration** > **Administrator Account Management**.
3. On the **Admin Accounts** tab, select the administrator accounts that you want to delete, and click **Delete**.

Creating an Admin Role

Procedure

1. Log on to the Mobile Security administration Web console.
2. Click **Administration** > **Administrator Account Management**.
3. On the **Admin Roles** tab, click **Create**.

   The **Create Admin Role** screen appears.

4. Under section **User Details**, provide the following information:

    - Admin Role

    - Description

5. Under section **Group Management Control** select the mobile device groups that this admin role can manage.

6. Click **Save**

Editing an Admin Role

Procedure

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

2. Click **Administration** > **Administrator Account Management**.

3. On the **Admin Roles** tab, click **Create**.

    The **Create Admin Role** screen appears.

4. Modify the role details as required and click **Save**.

Deleting an Admin Role

Procedure

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

2. Click **Administration** > **Administrator Account Management**.

3. On the **Admin Roles** tab, select the admin role you want to delete, and click **Delete**.

Changing Administrator Password

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

Command Queue Management

Mobile Security keeps the 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, navigate 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 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 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.

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 server IP address.
   - **HTTPS Port**—Mobile Security server HTTPS port number for the administration Web console.

Managing Certificates

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

Procedure

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

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

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)
- search for and display Mobile Device Agent status
- on-demand Mobile Device Agent component update, wipe/lock/locate remote device, and update policy
- configure Mobile Device Agents information
- export data for further analysis or backup

Groups in Mobile Security

Mobile Security 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 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".

Note

Device Authentication supports Android and iOS mobile devices only.

For instructions, refer to the Mobile Security 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. Type the **Group name** and 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 send invitation to mobile devices, edit mobile device information, delete mobile devices, or change the mobile device group on the **Devices** screen.

Sending Invitation to Mobile Devices

Procedure

1. Log on to the Mobile Securityadministration Web console.

2. Click **Devices** on the menu bar.

   The **Devices** screen displays.

3. You can now invite one mobile device, a batch of mobile devices, a user or an email group (distribution list) from the Active Directory:

- To invite a mobile device:

  a. Click **Invite Users** > **Invite Single User**.

     The **Invite Single User** window pops up.

  b. On the **Invite Single User** window, configure the following fields:

     - **Phone number**—type the phone number of a 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). You do not have to type the international direct dialing prefix.
     - **Email**—type the user email address to send notification mail.
     - **User Name**—type the name of the mobile device to identify the device in the tree.
     - **Group**—select the name of the group to which the mobile device belongs from the drop-down list. You can always change the group to which the mobile device agent belongs.

     Tip

     To invite more devices, click the ⊞ button.

- To invite a batch of mobile devices:

  a. Click **Invite Users** > **Invite Batch**.

  b. Type the device information using the following format in the text box on the window that displays:

     Phone_number, email_address, device_name, group_name, asset_number (optional), description(optional);

     Note

     Use semicolon (;) or "CR" to separate each device information.

  c. Click **Validate** to verify that the device information conforms to the specified format.

- To invite a user or an email group (distribution list) from the Active Directory:

  a. Click **Invite Users** > **Invite from Active Directory**.

  b. Type the user information in the search field provided, and click **Search**.

  c. Select the users from the search result, and then click **Invite Devices**.

4. Click **Save**.

Mobile Security sends invitation SMS or email to the users of the invited devices.

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). You do not have to type the international direct dialing prefix.

- **Email**—the user email address to send notification mail.

- **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 3-7*
- *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 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 server.

Moving Mobile Devices to Another Group

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

Procedure

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

2. Click **Devices** on the menu bar.

   The **Devices** screen displays.

3. On the **Managed Devices** tab, click the group whose mobile devices you want to move to another group.

4. Select the mobile devices from the list on the right pane and then click **Move**.

   The **Move Devices** dialog box displays.

5. From the drop-down list, select the target group and then click **OK**.

Mobile Device Status

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

- **Basic**—includes registration status, phone number, LDAP Account, and platform information.
- **Hardware, Operating System**—shows the detailed mobile device information including device and model names, operating system version, memory information, cellular technology, IMEI and MEID numbers, and firmware version information.
- **Security**—displays the mobile device's encryption status and whether the mobile device is jail broken or not.
- **Network**—displays the Integrated Circuit Card ID (ICCID), bluetooth and WiFi MAC information, detailed network information including carrier network name, settings version, roaming status, and Mobile Country Codes (MCC) and Mobile Network Codes (MNC) information.
- **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.

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 **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
   - **Asset Number**—asset number of a mobile device
   - **Description**— description of a mobile device
   - **Operating System**—operating system the mobile device is running
   - **Group**—group to which the mobile device belongs
   - **Agent Version**—Mobile Device Agents version number on the mobile device
   - **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
   - **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.

Device Tree View Options

If you select a group in the device tree, you can use the **Column** drop-down list box to select one of the pre-defined views: **General view** and **View all**. This enables you to quickly view information presented in the device tree. The information displayed in the device tree varies according to the selected option.

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 6-2* for more information.

On Windows Mobile or Symbian mobile devices, if you have not enabled the SMS messaging feature for Mobile Security, you need to configure update schedule in the **Common Policies** screen (see *Common Policy on page 4-7*) to periodically update components. However, on Android mobile devices, if you have not enabled the SMS messaging feature for Mobile Security, you can also update components and sync policies through push instructions.

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 Mobile Security server displays the mobile device location on Google Maps.

This feature is available for Android 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 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, iOS, BlackBerry and Windows Mobile devices only.

For Windows Mobile device to use this feature, the encryption must be enabled on the mobile device.

Windows Mobile device can only be locked using an SMS notification message. If you want to lock a Windows Mobile device, make sure you have configured an SMS sender. Refer to the *Installation and Deployment Guide* for the configuration details.

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. Click **Remote Lock** and then click **OK** on the confirmation dialog-box.

   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

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

WARNING!

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

Note

This feature is supported on Android, iOS, BlackBerry and Windows Mobile devices only.

For instructions on wiping a mobile device that uses Exchange ActiveSync, see *Wiping a Remote ActiveSync Mobile Device on page 3-22*.

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.** checkbox.

- 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, iOS and Windows 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.

Resetting Password for a Windows Mobile Device

To reset password for a Windows Mobile device, you will need to request user to generate a challenge code (16-digit hexadecimal number) on the mobile device before you can unlock the mobile device remotely.

Procedure

1. Obtain the mobile device name and the challenge code the user generated on the mobile device. Refer users to the Mobile Device Agent Help or the *User's Guide* for instructions on challenge code generation.
2. Log on to the Mobile Security administration Web console.
3. Click **Devices** on the menu bar.

   The **Devices** screen displays.
4. On the **Managed Devices** tab, click the mobile device from the device tree whose password you want to reset.

5. Click **Password Reset** and then click **Select a device** in the **Remote Unlock** screen. The device tree displays.

6. Select the mobile device you want to unlock remotely, and click **Select**.

7. Type the challenge code in the field and click **Generate**.

8. The Mobile Security server generates the response code and displays the code on a pop-up screen.

9. Instruct the user to tap **Next** in the **Password** screen on the mobile Device and type the response code to unlock the mobile device.

Exporting Data

On the **Managed Devices** tab in **Devices** screen, you can export data for further analysis or backup.

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.

Invited Devices Tab

The **Invited Devices** tab in **Devices** screen keeps the record the invitations that Mobile Security has sent to mobile devices for enrollment.

The default invitation email includes the following information:

- Trend Micro Mobile Security introduction
- Mobile Device Agent download URL
- Server information for mobile device to enroll
- QR code for easy enrollment

On the **Invited Devices** tab, you can:

- view the invitation list
- resend invitation messages to mobile devices
- cancel the current invitations
- remove the old invitation records

Viewing the Invitation List

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 **Invited Devices** tab.

   The following table provides the description of all the invitation statuses displayed on the **Invited Devices** tab.

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.

Resending Invitation Messages

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 **Invited Devices** tab.
4. Select the mobile devices from the list whom you want to resend the invitation message.
5. Click **Resend Invitation**.

Canceling Active Invitations

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 **Invited Devices** tab.
4. Select the mobile devices from the list for which you want to cancel the invitation.
5. Click **Cancel Invitation**.

Remove Invitations from the List

Note

You can only remove the invitation message whose status is **Used** or **Canceled**.

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 **Invited Devices** tab.
4. Select the mobile devices from the list whose invitation record you want to remove.
5. Click **Remove Invitation**.

Exchange ActiveSync Devices Tab

After enabling the Exchange Server Integration on the Mobile Security 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:

- Invite mobile devices
- Allow or block access to Exchange Server
- On-demand remote wipe
- Cancel remote wipe command
- Remove mobile devices from the list

Inviting Exchange ActiveSync Mobile Devices

Before inviting Exchange ActiveSync mobile devices, make sure that you have configured the notification/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 that you want to invite to access Exchange ActiveSync.
5. Click **Invite**, and then click **OK** on the confirmation screen.

Mobile Security sends invitation SMS and email messages to the user of the invited mobile device. After the mobile device enrolls to the Mobile Security 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

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.

WARNING!

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

For instructions on wiping a mobile device that does not use ActiveSync, see *Wiping a Remote Mobile Device on page 3-13*.

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 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 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.

Integration with Trend Micro Control Manager

Trend Micro Mobile Security provides integration with Trend MicroControl 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 MicroControl Manager and handling Mobile Securitypolicies 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

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:

- *Web Threat Protection Policy on page 4-17*
- *Encryption and Password Policy on page 4-19*
- *Feature Lock Policy on page 4-23*
- *Compliance Policy on page 4-24*
- *Application Monitor and Control Policy on page 4-24*
- *Volume Purchasing Program Policy on page 4-27*

About Security Policies

You can configure security policies for a Mobile Security group on the Management Server. These policies apply to all mobile devices in the group. You can apply security policies to all Mobile Security groups by selecting the **Mobile Devices** group (the root group). The following table lists the security policies available in Mobile Security.

TABLE 4-1. Security Policies in Mobile Security

POLICY GROUP	POLICY	REFERENCE
General	Common Policy	See *Common Policy on page 4-7*.
Provisioning	Wi-Fi Policy	See *Wi-Fi Policy on page 4-8*.
	Exchange ActiveSync Policy	See *Exchange ActiveSync Policy on page 4-9*.
	VPN Policy	See *VPN Policy on page 4-9*.
	Global HTTP Proxy Policy	See *Global HTTP Proxy Policy on page 4-9*.
	Certificate Policy	See *Certificate Policy on page 4-9*
Device Security	Malware Protection Policy	See *Malware Protection Policy on page 4-10*.
	Spam Prevention Policy	See *Spam Prevention Policy on page 4-11*.
	Call Filtering Policy	See *Call Filtering Policy on page 4-14*.
	Firewall Policy	See *Firewall Policy on page 4-16*.
	Web Threat Protection Policy	See *Web Threat Protection Policy on page 4-17*.

Policy Group	Policy	Reference
Devices	Encryption and Password Policy	See *Encryption and Password Policy on page 4-19*.
	Feature Lock Policy	See *Feature Lock Policy on page 4-23*.
	Compliance Policy	See *Compliance Policy on page 4-24*.
Application Management	Application Monitor & Control Policy	See *Application Monitor and Control Policy on page 4-24*.
	Volume Purchasing Program Policy	See *Volume Purchasing Program Policy on page 4-27*.

Managing Policies

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

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

Creating a Policy

Procedure

1. Log on to the Mobile Security administration Web console.
2. Click **Policies** 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 4-5*.

Editing a Policy

Procedure

1. Log on to the Mobile Security administration Web console.
2. Click **Policies** 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** 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** 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 4-5* for the procedure.

Procedure

1. Log on to the Mobile Security administration Web console.
2. Click **Policies** on the menu bar.

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

Security Policies in Mobile Security

This section introduces the security policies that are available in Mobile Security.

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**.

In **Common Policy** you can also assign policies for BlackBerry mobile devices.

- **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:

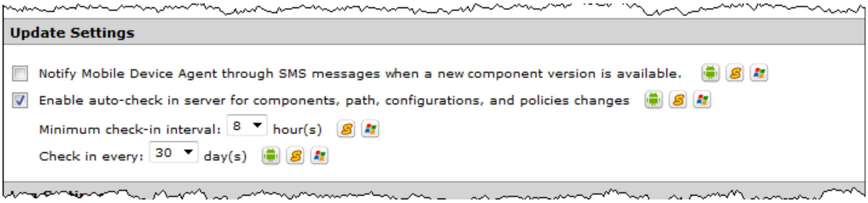
  - turn On/Off uninstall protection from the administration console
  - password length must have a minimum of six (6) and a maximum of twelve (12) characters; password may contain numbers, characters or symbols.
  - password can be set for each group from the administration console.

  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 4-11*, *Spam WAP-Push Prevention Policies on page 4-13* and *Web Threat Protection Policy on page 4-17*.

- **Update Settings**: You can select to have the Mobile Security 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 server.

  When you enable the wireless connection notification option, a prompt screen displays on mobile devices before Mobile Device Agents connect to the

Communication Server through a wireless connection (such as 3G or GPRS). Users can choose to accept or decline the connection request.



Update Settings

□ Notify Mobile Device Agent through SMS messages when a new component version is available.

☑ Enable auto-check in server for components, path, configurations, and policies changes

Minimum check-in interval: 8 hour(s)

Check in every: 30 day(s)

FIGURE 4-1. Common Policy, Update Settings section

- **Log Settings**: When Mobile Device Agents detect a security risk, such as an infected file or firewall violation, a log is generated on mobile devices. If the Encryption Module is activated, the encryption logs are also generated. You can set the mobile devices to send these logs to the Mobile Security server. Do this if you want to analyze the number of infections or pinpoint possible network attacks and take appropriate actions to prevent threats from spreading.

- **Notification/Reports Settings**: Select whether to display a prompt screen on mobile devices when a mobile device agent tries to establish a connection to the Communication Server.

- **BlackBerry Settings**: Enables you to configure common policy settings for BlackBerry mobile devices.

Note

You must configure the BlackBerry Settings in the Communication Server settings before you can configure the policy settings. Refer to the topic *Configuring BlackBerry Communication Server Settings* in the *Installation and Deployment Guide.*

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 enables 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**.

Malware Protection Policy

You can configure threat protection policies that include: Scan type (real-time and card scan), action taken for malware, number of compression layers to scan, and the File type.

To configure malware protection policy settings, click **Policies**, then click the policy name, and then click **Malware Protection Policy**.

- **Scan Types**: Mobile Security provides several types of scans to protect mobile devices from malware.
  - **Real-time Scan**: Mobile Device Agent scans files on mobile devices in real time. If Mobile Device Agent detects no security risk, users can proceed to open or save the file. If Mobile Device Agent detects a security risk, it displays the scan result, showing the name of the file and the specific security risk. Mobile Security will generate a log with the scan result on the mobile device. The scan log is sent and stored on the Mobile Security database.
  - **Scan after SD card insert**: If you select this option in the **Malware Protection Policy** screen, Mobile Security scans data on a memory card when the memory card is inserted to a mobile device. This prevents infected files from spreading through memory cards.
  - **Scan after pattern update**: If you select the this option in the **Malware Protection Policy** screen, Mobile Security will run an automatic-scan for security threats after successful pattern update on Android mobile devices.
- **Scan Options**
  - **Action on malware**: When malware is detected on a mobile device, Mobile Security can delete or quarantine the infected file. If the file is in use, the operating system may deny access to it.
    - Quarantine—renames and then moves an infected file to the mobile device's quarantine directory in`\TmQuarantine` (for Windows Mobile) or `{Disk Label}\TmQuarantine` (for Symbian OS).
    - Delete—removes an infected file.

    When connected, Mobile Device Agents send malware logs to the Mobile Security server.

Note

Scan actions only apply to Real-time scan.

- **Compression layers to scan**: For ZIP or CAB files, you can specify the number of compression layers to scan. If the number of compression in a ZIP/CAB file exceeds this number, Mobile Security will not scan the file. Mobile Security will take no further action unless the appropriate number of compression layers are specified.

  You can select to have Mobile Security scan executable, ZIP/CAB files, or all files on mobile devices.

- **Scan Location**: For Android mobile devices, select whether to scan mobile device's internal memory and/or the inserted SD card. For SymbianMobile Security scans both the mobile device's internal memory and the inserted SD card.

- **File type**: Select the file types to scan on mobile devices.

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

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 4-2. 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
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

This feature provides you server-side control of WAP-Push Protection. If enabled, you can select whether to use a WAP approved list. The following features is a list of features available when configuring WAP-Push Protection policies:

- enable or disable WAP-Push protection for mobile device
- configure the mobile device to use an approved list or disable WAP-Push protection 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 protection 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 protection list configured by the administrator, and may edit the personal WAP-Push protection list on the mobile device side

The personal settings will be cleared after server policy is delivered to a mobile device.

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.

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

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 4-3. 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.

Firewall Policy

The Mobile Security firewall protects mobile devices on the network using stateful inspection, high performance network traffic control and the intrusion detection system (IDS). You can create rules to filter connections by IP address, port number, or protocol, and then apply the rules to mobile devices in specific Mobile Security groups.

Note

Trend Micro recommends uninstalling other software-based firewall applications on mobile devices before deploying and enabling Mobile Security firewall. Multiple vendor firewall installations on the same computer may produce unexpected results.

To configure firewall policy settings, click **Policies**, then click the policy name, and then click **Firewall Policy**.

A firewall policy includes the following:

- **Firewall Policy**: Enable/Disable the Mobile Security firewall and the IDS. Also includes a common policy that blocks or allows all inbound and/or all outbound traffic on mobile devices
    - **Enable Intrusion Detection System (IDS)**: The Mobile Security firewall integrates the Intrusion Detection System (IDS) and helps prevent SYN Flood attacks (a type of Denial of Service attack) where a program sends multiple TCP synchronization (SYN) packets to a computer, causing the mobile device to continually send synchronization acknowledgment (SYN/ ACK) responses. This can exhaust system resource and may leave mobile devices unable to handle other requests.
    - **Security level**: The Mobile Security firewall comes with three pre-defined security levels that allow you to quickly configure firewall policies. These security levels limit network traffic based on traffic directions.
        - **Low**—allow all inbound and outbound traffic.
        - **Normal**—allow all outbound traffic but block all inbound traffic.
        - **High**—block all inbound and outbound traffic.

- **Exception**: Exception rules include more specific settings to allow or block different kinds of traffic based on mobile device port number(s) and IP address(es). The rules in the list override the **Security level** policy.

  Exception rule settings include the following:

  - **Action**—blocks or allows/logs traffic that meets the rule criteria
  - **Direction**—inbound or outbound network traffic on mobile devices
  - **Protocol**—type of traffic: TCP, UDP, ICMP
  - **Port(s)**—ports on the mobile devices on which to perform the action
  - **IP addresses**—IP addresses of network devices to which the traffic criteria apply

Web Threat Protection Policy

Enables you to manage Web threat protection policy from the Mobile Security server and deploys it on Android mobile devices. It also enables Android mobile devices to send the Web threat protection log back to the server.

This feature provides you the server-side control of Web threat protection policies and provides three pre-defined security levels: **Low**, **Normal**, and **High**. It also provides blocked and approved lists to block or allow certain URLs. Mobile Security will block all the URLs that you add in the Blocked List, and allow all URLs that are in the Approved List.

Note

The Web threat protection policy only supports Google Chrome and Android's default Web browser on mobile devices.

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

TABLE 4-4. Filtering list configuration for Web Threat Protection policy

SERVER 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
Enabled	Disabled	The user is only allowed to 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 server 2. Blocked List on server 3. Approved List on Mobile Device Agent 4. Blocked List on Mobile Device Agent
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 URLs based on the following priority: 1. Approved List on Mobile Device Agent 2. Blocked List on Mobile Device Agent 3. Approved List on server 4. Blocked List on server

Note

The call filtering approved and blocked lists must use the following format: [URL1] [URL2] [URL3], with a blank space or a line break between two URLs.

To configure Web Threat Protection Policy settings, click **Policies**, then click the policy name, and then click **Web Threat Protection Policy**.

Encryption and Password Policy

The encryption and password module provides password authenticating and data encryption on mobile devices. These features prevent unauthorized access to data on mobile devices.

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

Password Security Settings

When Mobile Device Agent is installed, each mobile device is associated with a user. The user must type the correct power-on password to log on to the mobile device. When a user has forgotten the power-on password, you can type the administrator password to unlock a mobile device.

The following table describes the power-on password policies you can configure:

OPTION	DESCRIPTION
Password type	Passwords must contain only numbers or alphanumeric characters.
Minimum password length	Passwords must be longer than the number of characters specified.
Password complexity	For alphanumeric passwords, users must configure passwords that contain upper case, lower case, special characters, or numbers to make passwords harder to guess.

OPTION	DESCRIPTION
Initial Mobile Device Agent password	Password that allows users to log on to their Windows Mobile devices after installing the Mobile Device Agent and the Encryption Module. The default is "123456".
Admin password	Password used by an administrator to unlock a mobile Device.
Expiry period	The number of days a logon password is valid. After the password expires, the user must configure a new password to log on.
Inactivity timeout	The number of minutes of no user activity before the mobile device automatically goes into secure mode and display the logon screen.
Limit logon attempts	Limit the number of logon attempts to prevent brute force password attack. Possible actions when the limit is reached: • **Soft reset**—restarts the mobile device. • **Admin access only**—requires logon using the administrator password. • **Hard reset**—resets the mobile device back to the factory default policies. • **Clear all data**—resets the mobile device back to the factory default policies and deletes all the data on the mobile device and the inserted memory card. **WARNING!** After a "Clear all data" action, users need to reformat the memory card to use it again for storing data.
Change initial power-on password	Request users to change the initial password after the first logon.
Forgotten password questions	If a user has forgotten the power-on password, this feature allows the user to unlock mobile devices and configure a new password by answering the selected question.

Note

When specifying the characters for the initial or admin password, keep in mind the input method used by mobile devices. Otherwise, the device user may not be able to unlock the device after encryption is enabled.

Encryption Settings

Mobile Device Agent provides on-the-fly data encryption function to secure data on mobile devices. Two encryption algorithms are available: Advanced Encryption Standard (AES, with 128-bit, 192-bit, or 256-bit keys) and XTS-Advanced Encryption Standard (AES).

Note

Mobile Security can only manage the data security policy on Windows Mobile devices.

You can select specific file types to encrypt on Windows Mobile devices, the encryption algorithm to use, trusted applications that are allowed to access encrypted data, or apply data encryption on memory cards inserted on mobile devices.

Mobile Device Agent does not encrypt Dynamic Link Library (`*.DLL`) files. Mobile Device Agent only encrypts files that a user has modified. Reading a file and closing it without any modifications does not result in the file being encrypted.

After the Encryption Module is enabled, certain file types and PIM information are encrypted. These file types and PIM Information are listed in the following table.

Encrypted Information	Types
File Types	• `doc` • `txt` • `ppt` • `pxl` • `pdf` • `xls` • `psw` • `docx`
PIM Information	• Contacts • Mail • Tasks • Calendar • SMS • MMS

The Encryption Module only allows trusted applications to access encrypted data. Therefore, you must add these applications to the trusted application list. To add software to the trusted application list, add the full software path to the appropriate list under: "**Allow more applications to access encrypted data**".

Note

For advanced configuration, you can set Mobile Security to encrypt other file types. To enable encryption of custom file types, set the parameter **Enable_Custom_Extension** to `1` in the file `TmOMSM.ini` (located in `\Trend Micro\Mobile Security`). When the parameter is set to **"1"** in the file `TmOMSM.ini`, the **Encrypt other file types** field displays in the **Data Security Policies** screen. Specify the file types in this field.

To disable this feature, set the parameter **Enable_Custom_Extension** to `0`. When the parameter is set to **"0"** in the file `TmOMSM.ini`, the **Encrypt other file types** field is not available in the **Data Security Policies** screen.

After making the change in the `TmOMSM.ini` file, restart **Mobile Security Management Module Service** service for the change to take effect.

WARNING!

Trend Micro does not recommend customizing file types for encryption. You cannot encrypt certain files types (for example, `.exe`, `.cert`, `.dll`, etc.). If you set Mobile Security to encrypt file types that should not be encrypted, unexpected system errors may occur.

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.

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 1-15* for the list of supported features/ components.

Note

The Feature Lock Policy is NOT available for Symbian mobile devices.

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).

Note

Windows Mobile devices may need to reboot for changes to take effect.

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**—selecting this option will push all the applications that you add in the list, to the mobile devices.
- **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.
  - Mobile Security displays a pop-up warning message on Android mobile devices if it detects applications that are in the blocked list.
- **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 5-2* 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.

Chapter 5

Managing Enterprise App Store

This chapter shows you how to manage the store for enterprise applications for iOS and Android mobile devices.

The chapter includes the following sections:

About 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 Applications

Adding an Application

Procedure

1. Log on to the Mobile Security administration Web console.
2. Click **App Store** on the menu bar.

   The **Enterprise App Store** screen displays.
3. Click the **iOS Applications** tab or **Android Applications** tab.
4. Click **Add**.

   The **Add Application** window displays.
5. 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) **Please input search keyword**—type the name of the VPP application you want to search 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 4-27* for the procedure.

6. Click **Continue**.

   The **Edit Application** screen displays.

7. 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.

8. Click **Continue**.

   The application appears in the applications list.

Editing Application Information

Procedure

1. Log on to the Mobile Security administration Web console.
2. Click **App Store** on the menu bar.

   The **Enterprise App Store** screen displays.
3. Click the **iOS Applications** tab or **Android Applications** tab.
4. Click the application name whose information you want to edit.

   The **EditApplication** window displays.
5. Modify the details on the screen.
6. Click **Continue**.

Deleting Applications from the App Store

Procedure

1. Log on to the Mobile Security administration Web console.
2. Click **App Store** on the menu bar.

The **Enterprise App Store** screen displays.

3. Click the **iOS Applications** tab or **Android Applications** tab.
4. Select the applications that you want to delete.
5. Click **Delete** and then click **OK** on the confirmation dialog box.

Managing Application Categories

Adding an Application Category

Procedure

1. Log on to the Mobile Security administration Web console.
2. Click **App Store** on the menu bar.

   The **Enterprise App Store** screen displays.
3. Click the **iOS Applications** tab or **Android Applications** tab.
4. Click **Manage Category**.
5. Click **Add**.

   The **Add Category** window displays.
6. Type the category name and description and then click **Save**.

Editing an Application Category

Procedure

1. Log on to the Mobile Security administration Web console.
2. Click **App Store** on the menu bar.

The **Enterprise App Store** screen displays.

3. Click the **iOS Applications** tab or **Android Applications** tab.

4. Click **Manage Category**.

5. Click the category name that you want to edit.

   The **Edit Category** window displays.

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

Deleting an Application Category

Procedure

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

2. Click **App Store** on the menu bar.

   The **Enterprise App Store** screen displays.

3. Click the **iOS Applications** tab or **Android Applications** tab.

4. Click **Manage Category**.

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

Chapter 6

Updating Components

This chapter shows you how to configure scheduled and manual server updates and then specify the update source for ActiveUpdate. You will also learn to perform component updates on specific Mobile Device Agents.

The chapter includes the following sections:

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 server.
- Malware Pattern—file containing thousands of malware signatures, and determines Mobile Security's ability to detect these hazardous files. Trend Micro updates pattern files regularly to ensure protection against the latest threats.
- Malware Scan Engine—component that performs the actual scanning and cleaning functions. The scan engine employs pattern-matching technology, using signatures in the pattern file to detect malware. Trend Micro occasionally issues a new scan engine to incorporate new technology.
- Mobile Device Agents installation program—program installation package for the Mobile Device Agents.
- Mobile Device Agent program patch—program patch file that includes the latest updates to the Mobile Device Agent program installed on mobile devices.

Updating Mobile Security Components

You can configure scheduled or manual component updates on the Mobile Security server to obtain the latest component files from the ActiveUpdate server. After a newer version of a component is downloaded on Mobile Security server, the Mobile Security 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 6-5* for more information).

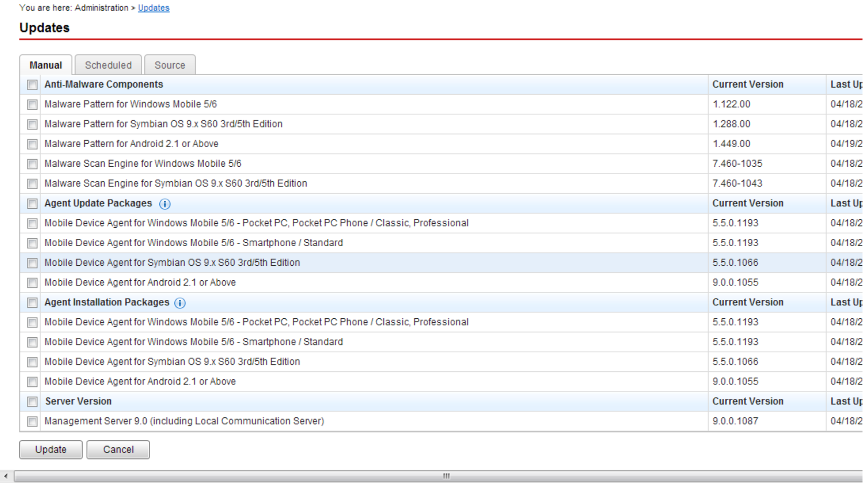
Procedure

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

2. Click **Administration** > **Updates**.

   The **Updates** screen displays.

3. Click the **Manual** tab.



You are here: Administration > Updates

Updates

□	**Anti-Malware Components**	**Current Version**	**Last Up**
□	Malware Pattern for Windows Mobile 5/6	1.122.00	04/18/2
□	Malware Pattern for Symbian OS 9.x S60 3rd/5th Edition	1.288.00	04/18/2
□	Malware Pattern for Android 2.1 or Above	1.449.00	04/19/2
□	Malware Scan Engine for Windows Mobile 5/6	7.460-1035	04/18/2
□	Malware Scan Engine for Symbian OS 9.x S60 3rd/5th Edition	7.460-1043	04/18/2
□	**Agent Update Packages** ⓘ	**Current Version**	**Last Up**
□	Mobile Device Agent for Windows Mobile 5/6 - Pocket PC, Pocket PC Phone / Classic, Professional	5.5.0.1193	04/18/2
□	Mobile Device Agent for Windows Mobile 5/6 - Smartphone / Standard	5.5.0.1193	04/18/2
□	Mobile Device Agent for Symbian OS 9.x S60 3rd/5th Edition	5.5.0.1066	04/18/2
□	Mobile Device Agent for Android 2.1 or Above	9.0.0.1055	04/18/2
□	**Agent Installation Packages** ⓘ	**Current Version**	**Last Up**
□	Mobile Device Agent for Windows Mobile 5/6 - Pocket PC, Pocket PC Phone / Classic, Professional	5.5.0.1193	04/18/2
□	Mobile Device Agent for Windows Mobile 5/6 - Smartphone / Standard	5.5.0.1193	04/18/2
□	Mobile Device Agent for Symbian OS 9.x S60 3rd/5th Edition	5.5.0.1066	04/18/2
□	Mobile Device Agent for Android 2.1 or Above	9.0.0.1055	04/18/2
□	**Server Version**	**Current Version**	**Last Up**
□	Management Server 9.0 (including Local Communication Server)	9.0.0.1087	04/18/2

FIGURE 6-1. The Manual tab on Updates screen

4. Select the check box of the component you want to update. Select the **Anti-Malware Components**, **Program** and/or **Program Installation Package** 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 6-2* for more information on each update component.

5. Click **Update** to start the component update process.

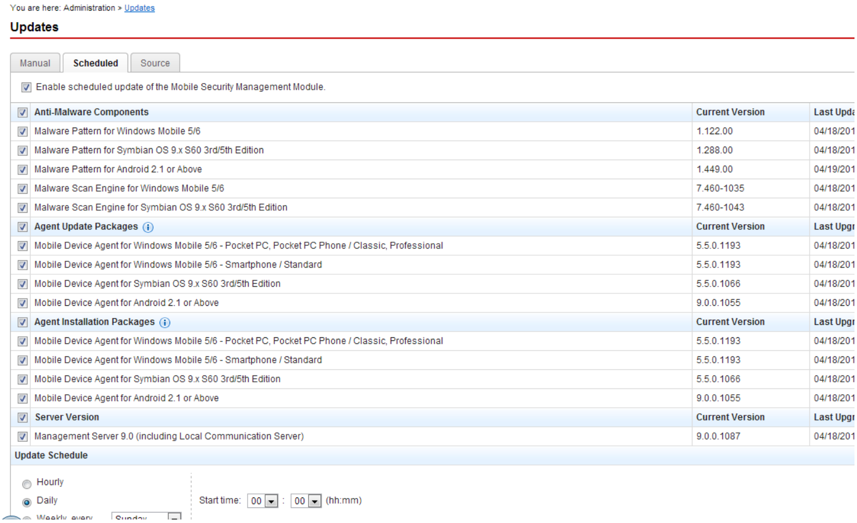
Scheduled Update

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 6-5* 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.



You are here: Administration > Updates

Updates

☑ Enable scheduled update of the Mobile Security Management Module.

☑ Anti-Malware Components	Current Version	Last Upda
☑ Malware Pattern for Windows Mobile 5/6	1.122.00	04/18/201
☑ Malware Pattern for Symbian OS 9.x S60 3rd/5th Edition	1.288.00	04/18/201
☑ Malware Pattern for Android 2.1 or Above	1.449.00	04/19/201
☑ Malware Scan Engine for Windows Mobile 5/6	7.460-1035	04/18/201
☑ Malware Scan Engine for Symbian OS 9.x S60 3rd/5th Edition	7.460-1043	04/18/201
☑ **Agent Update Packages** ⓘ	**Current Version**	**Last Upgr**
☑ Mobile Device Agent for Windows Mobile 5/6 - Pocket PC, Pocket PC Phone / Classic, Professional	5.5.0.1193	04/18/201
☑ Mobile Device Agent for Windows Mobile 5/6 - Smartphone / Standard	5.5.0.1193	04/18/201
☑ Mobile Device Agent for Symbian OS 9.x S60 3rd/5th Edition	5.5.0.1066	04/18/201
☑ Mobile Device Agent for Android 2.1 or Above	9.0.0.1055	04/18/201
☑ **Agent Installation Packages** ⓘ	**Current Version**	**Last Upgr**
☑ Mobile Device Agent for Windows Mobile 5/6 - Pocket PC, Pocket PC Phone / Classic, Professional	5.5.0.1193	04/18/201
☑ Mobile Device Agent for Windows Mobile 5/6 - Smartphone / Standard	5.5.0.1193	04/18/201
☑ Mobile Device Agent for Symbian OS 9.x S60 3rd/5th Edition	5.5.0.1066	04/18/201
☑ Mobile Device Agent for Android 2.1 or Above	9.0.0.1055	04/18/201
☑ **Server Version**	**Current Version**	**Last Upgr**
☑ Management Server 9.0 (including Local Communication Server)	9.0.0.1087	04/18/201

Update Schedule

○ Hourly

● Daily — Start time: 00 : 00 (hh:mm)

○ Weekly, every Sunday

FIGURE 6-2. The Scheduled tab on Updates screen

4. Select the check box of the component you want to update. Select the **Anti-Malware Components**, **Agent Update Packages**, **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 schedules, specify the day of the week (for example, Sunday, Monday, and so on.)

   - For monthly schedules, 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 x 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.

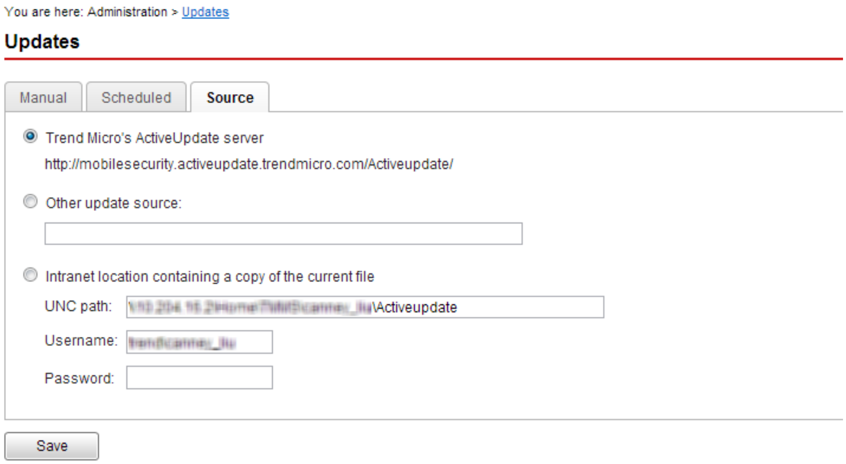
Procedure

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 6-2* or for scheduled update see *Scheduled Update on page 6-4*.

3. Click the **Source** tab.



You are here: Administration > Updates

Updates

● Trend Micro's ActiveUpdate server

http://mobilesecurity.activeupdate.trendmicro.com/Activeupdate/

○ Other update source:

○ Intranet location containing a copy of the current file

UNC path: [redacted]\Activeupdate

Username: [redacted]

Password:

FIGURE 6-3. The Source tab on Updates screen

4. Select one of the following download sources:

   - **Trend Micro ActiveUpdate server**—the default update source.
   - **Other update source**—specify HTTP or HTTPS Web site (for example, your local Intranet Web site), 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 Mobile Security 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 7

Viewing and Maintaining Logs

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

The chapter includes the following sections:

About Mobile Device Agent Logs

When Mobile Device Agents generate a malware protection log, Web threat protection log, firewall log, encryption log, policy violation log or an event log, the log is sent to the Mobile Security 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 server. On the Mobile Security server, you can view the following Mobile Device Agent logs:

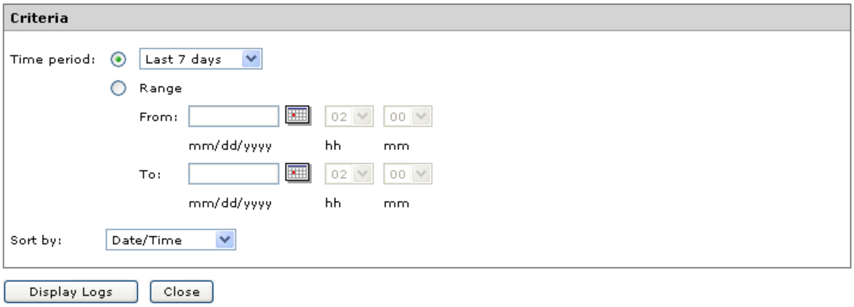
- Malware Protection Log—Mobile Device Agent generates a log when a malware is detected on the mobile device. These logs allow you to keep track of the malware that were detected and the measures taken against them.
- Web Threat Protection Log—Mobile Security Agent generates a log when it blocks a dangerous or malware-infected Web page, and upload the log to server.
- Firewall Log—these logs are generated when a firewall rule is matched or when the firewall feature (such as the predefined security level or IDS) blocks a connection.
- Encryption Log—include information such as successful user logon attempts and actions taken after reaching the logon attempt limit.
- Event Log—these logs are generated when certain actions are taken by the server and the Mobile Device Agent.
- Policy Violation Log—these logs include information about the policy compliant status of Mobile Device Agents.

Procedure

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

2. Click **Notifications & Reports** > **Log Query**.

   The **Log Query** screen displays.



Criteria

Time period: ● Last 7 days

○ Range

From: mm/dd/yyyy 02 hh 00 mm

To: mm/dd/yyyy 02 hh 00 mm

Sort by: Date/Time

FIGURE 7-1. 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.

   - **Admin name**—type the administrator name whose generated logs you want to search.

   - **Time period**—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. Log on to the Mobile Security administration Web console.
2. Click **Notifications & Reports** > **Log Maintenance**.

   The **Log Maintenance** screen displays.
3. Select **Enable scheduled deletion of logs**.
4. Select the log types to delete: Malware, Firewall, Encryption, Event or Policy Violation.
5. Select whether to delete logs for all the selected log types or those older than the specified number of days.
6. Specify the log deletion frequency and time.
7. Click **Save**.

Deleting Logs Manually

Procedure

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

   The **Log Maintenance** screen displays.
3. Select the log types to delete.
4. Select whether to delete logs for all the selected log types or only older than the specified number of days.
5. Click **Delete Now**.

Chapter 8

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

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

- **Administrator Notifications/Reports**—sends email notifications and reports to the administrator in case any system abnormality occurs.
- **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. Log on to the Mobile Security administration Web console.
2. Click **Notifications & Reports** > **Settings**.

   The **Notifications/Reports Settings** screen displays.
3. Under **Email Settings** section, type the **From** email address, the SMTP server IP address and its port number.
4. If the SMTP server requires authentication, select **Authentication**, and then type the username and password.
5. Click **Save**.

Related information

↳ *Configuring SMS Sender List*

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 and Scheduled Reports on page 8-7* 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 and Scheduled Reports

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

- Notifications:

  - **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's name in the email.
  - **APNS Certificate Expired Warning**—sends email notification to administrator when the APNs certificate expires.
- Reports:
  - **Devices Inventory Report**—is the comprehensive report of all the mobile devices managed by Mobile Security.
  - **Compliance Violation Report**—is the report of all the mobile devices managed by Mobile Security that do not comply with the configured policy.
  - **Malware Detection Report**—is the report of all the security threats detected on mobile devices managed by Mobile Security.
  - **Web Threat Protection Report**—is the report of all the unsafe URLs accessed on mobile devices managed by Mobile Security.
  - **Application Inventory Report**—is the report of all the apps installed on mobile devices managed by Mobile Security.
  - **Devices Enrollment Report**—is the report of mobile devices enrollment information managed by Mobile Security.
  - **Devices Decommission Report**—is the report of mobile devices decommission information managed by Mobile Security.
  - **Policy Violation Report**—is the report of mobile devices that violate the security policies.

Configuring Administrator Notifications

Procedure

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

   The **Notifications/Reports Settings** screen displays.
3. Select the notifications and reports you want to receive via email, and then click on individual notifications and reports to modify their contents.

   Note

   When you select reports that you want to receive, you can also adjust their frequencies individually from the drop-down list after each report.

   Note

   While editing the **Message** field in email notification messages, make sure to include the token variables `<%PROBLEM%>`, `<%REASON%>` and `<%SUGGESTION%>`, which will be replaced by the actual values in the email message.
4. Click **Save** when done, to return back to the **Administrator Notifications/ Reports** screen.

User Notification

Use the **User Notifications** screen to configure the following email and/or SMS text 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.

Configuring User Notifications

Procedure

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

   The **Notifications/Reports Settings** screen displays.
3. 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.

     Note

     While editing the **Message** field, make sure to include the token variables <%DOWNLOADURL%> or <%DEVICE_NAME%> and <%VIOLATION%>, which will be replaced by the actual URLs in the email message.
   - To configure text notification messages, update the body of the message in the **Message** field.

     Note

     While editing the **Message** field, make sure to include the token variables <%DOWNLOADURL%>, which will be replaced by the actual URL in the text message.

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

Chapter 9

Troubleshooting and Contacting Technical Support

Here you will find answers to frequently asked questions and you learn how to obtain additional Mobile Security information.

The chapter includes the following sections:

Troubleshooting

This section provides tips for dealing with issues you may encounter when using Mobile Security.

- **User cannot input nanoscale passwords on their devices.**

  Mobile device keypads can only support a certain set of characters. Mobile Security recommends that the administrator compile a list of characters supported by the devices. After compiling the list of supported characters, the administrator can then set the uninstall protection password from the management console using the list of supported characters.

- **The Mobile Device Agent cannot receive the server's SMS notification or connect to the server via the public DNS name.**

  The version of Mobile Device Agent supporting a DNS name should be higher than 5.0.0.1099 for Windows Mobile platform and higher than 5.0.0.1061 for Symbian OS 9.x S60 3rd Edition platform. Previous versions can connect via IP address only.

- **Application(s) fail to function after enabling Encryption Module.**

  When a user uses the Encryption Module on a device, some existing applications may not function. The reason is that these existing applications may be not be contained in the trusted list. After the Encryption Module is enabled, certain file types will be encrypted (for example, `doc`, `txt`, `ppt`, `pdf`, `xls` and etc). The Encryption Module only allows trusted applications to access encrypted data. Therefore, the administrator must add these applications to the trusted application list. For more information see *Encryption Settings on page 4-21*.

- **After canceling the Communication Server uninstallation process, the Communication Server fails to function normally.**

  If the uninstallation process started deleting the files and services that are important for the Communication Server's normal operation before the process was stopped, the Communication Server may not function normally. To resolve this issue, install and configure the Communication Server again.

- **iOS mobile devices cannot enroll successfully to the Management Server, and displays "Unsupported URL" error message.**

This issue may happen if the system clock of SCEP server is set to the incorrect time or the Simple Certificate Enrollment Protocol (SCEP) certificate is not obtained by Trend Micro Mobile Security. Make sure that the system clock of SCEP server is set to the correct time. If the issue persists, perform the following steps:

1. Log on to the Mobile Security administration Web console.
2. Click **Administration** > **Communication Server** Settings.
3. Without changing the settings, click **Save**.

- **The Management Server cannot receive policy from the BlackBerry Enterprise Server (BES).**

  The Communication Server cannot receive the policy from the BlackBerry Enterprise Server (BES) if the policy name contains special characters. Check if the policy name contain any special characters and replace them with alphabets and numbers.

- **Unable to save Database Settings if you use SQL Server Express.**

  If you are using SQL Server Express, use the following format in the Server address field: `<SQL Server Express IP address>\sqlexpress`.

  Note

  Replace `<SQL Server Express IP address>` with the IP address of SQL Server Express.

- **Unable to connect to SQL Server 2005 or SQL Server 2005 Express.**

  This problem may occur when SQL Server 2005 is not configured to accept remote connections. By default, SQL Server 2005 Express Edition and SQL Server 2005 Developer Edition do not allow remote connections. To configure SQL Server 2005 to allow remote connections, complete all the following steps:

  1. Enable remote connections on the instance of SQL Server that you want to connect to from a remote computer.
  2. Turn on the SQL Server Browser service.

3. Configure the firewall to allow network traffic that is related to SQL Server and to the SQL Server Browser service.

- **Unable to connect to SQL Server 2008 R2.**

  This problem may occur if Visual Studio 2008 is not installed in the default location and therefore, the SQL Server 2008 setup cannot find devenv.exe.config configuration file. To resolve this issue, perform the following steps:

  1. Go to `<Visual Studio installation folder>\Microsoft Visual Studio 9.0\Common7\IDE` folder, find and copy `devenv.exe.config` file and paste it to the following folder (you may need to enable display extensions for known file types in folder options):

     - For 64-bit Operating System:

       ```
       C:\Program Files (x86)\Microsoft Visual Studio
       9.0\Common7\IDE
       ```

     - For 32-bit Operating System:

       ```
       C:\Program Files\Microsoft Visual Studio
       9.0\Common7\IDE
       ```

  2. Run the SQL Server 2008 setup again and add BIDS feature to the existing instance of SQL Server 2008.

- **Unable to export the client device list in Device Management.**

  This may occur if the downloading of encrypted files is disabled in the Internet Explorer. Perform the following steps to enable the encrypted files download:

  1. On your Internet Explorer, go to **Tools** > **Internet options**, and then click the **Advanced** tab on the **Internet Options** window.

  2. Under **Security** section, clear **Do not save encrypted pages to disk**.

  3. Click **OK**.

- **The status of certain Android mobile device is always Out of Sync.**

  This is because the Mobile Security device administrator is not activated on that mobile device. If the user does not activate Mobile Security in the Device administrators list, then the Mobile Security cannot synchronize server policies with the mobile device, and displays its status as Out of Sync.

- **The content on the Policy pop-up window does not display and is blocked by Internet Explorer.**

  This happens if your Internet Explorer is configured to use a .pac automatic configuration file. In that case, the Internet Explorer will block the access to a secure Web site that contains multiple frames. To resolve this issue, add the Mobile Security server address to the Trusted sites security zone in Internet Explorer. To do this, perform the following steps:

  1. Start Internet Explorer.
  2. Go to **Tools** > **Internet options**.
  3. On the **Security** tab, click **Trusted sites**, and then click **Sites**.
  4. In the **Add this Web site to the zone** text field, type the Mobile Security server URL, and then click Add.
  5. Click **OK**.

  For more details on this issue, refer to the following URL:

  http://support.microsoft.com/kb/908356

Before Contacting Technical Support

Before contacting technical support, here are two things you can quickly do to try and find a solution to your problem:

- **Check your documentation**—The manual and online help provide comprehensive information about Mobile Security. Search both documents to see if they contain your solution.
- **Visit our Technical Support Web site**—Our Technical Support Web site, called Knowledge Base, contains the latest information about all Trend Micro products. The support Web site has answers to previous user inquiries.

  To search the Knowledge Base, visit

http://esupport.trendmicro.com

Contacting Technical Support

Trend Micro provides technical support, pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

- Get a list of the worldwide support offices at *http://esupport.trendmicro.com*
- Get the latest Trend Micro product documentation at *http://docs.trendmicro.com*

In the United States, you can reach the Trend Micro representatives through phone, fax, or email:

Trend Micro, Inc.
10101 North De Anza Blvd.,
Cupertino, CA 95014
Toll free: +1 (800) 228-5651 (sales)
Voice: +1 (408) 257-1500 (main)
Fax: +1 (408) 257-2003
Web address: *http://www.trendmicro.com*
Email: *support@trendmicro.com*

Sending Infected Files to Trend Micro

You can send malware and other infected files to Trend Micro. More specifically, if you have a file that you think is some kind of malware but the scan engine is not detecting it or cleaning it, you can submit the suspicious file to Trend Micro using the following address:

http://esupport.trendmicro.com/srf/srfmain.aspx

Please include in the message text a brief description of the symptoms you are experiencing. Our team of malware engineers will "dissect" the file to identify and characterize any malware it may contain and return the cleaned file to you, usually within 48 hours.

TrendLabs

Trend Micro TrendLabs℠ is a global network of antivirus research and product support centers providing continuous, 24 x 7 coverage to Trend Micro customers worldwide.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers worldwide ensure rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters earned ISO 9002 certification for its quality management procedures in 2000. TrendLabs is one of the first antivirus research and support facilities to be so accredited. Trend Micro believes that TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:

http://us.trendmicro.com/us/about/company/trendlabs/

About Software Updates

After a product release, Trend Micro often develops updates to the software, to enhance product performance, add new features, or address a known issue. There are different types of updates, depending on the reason for issuing the update.

The following is a summary of the items Trend Micro may release:

- **Hot fix**—A hot fix is a workaround or solution to a single customer-reported issue. Hot fixes are issue-specific, and therefore not released to all customers. Windows hot fixes include a Setup program, while non-Windows hot fixes do not (typically you need to stop the program daemons, copy the file to overwrite its counterpart in your installation, and restart the daemons).
- **Security Patch**—A security patch is a hot fix focusing on security issues that is suitable for deployment to all customers. Windows security patches include a Setup program, while non-Windows patches commonly have a setup script.

- **Patch**—A patch is a group of hot fixes and security patches that solve multiple program issues. Trend Micro makes patches available on a regular basis. Windows patches include a Setup program, while non-Windows patches commonly have a setup script.
- **Service Pack**—A service pack is a consolidation of hot fixes, patches, and feature enhancements significant enough to be considered a product upgrade. Both Windows and non-Windows service packs include a Setup program and setup script.

Check the Trend Micro Knowledge Base to search for released hot fixes:

http://esupport.trendmicro.com

Consult the Trend Micro Web site regularly to download patches and service packs:

http://www.trendmicro.com/download

All releases include a readme file with the information needed to install, deploy, and configure your product. Read the readme file carefully before installing the hot fix, patch, or service pack file(s).

Known Issues

Known issues are features in Mobile Security that may temporarily require a workaround. Known issues are typically documented in the Readme document you received with your product. Readmes for Trend Micro products can also be found in the Trend Micro Download Center:

http://www.trendmicro.com/download/

Known issues can be found in the technical support Knowledge Base:

http://esupport.trendmicro.com

Trend Micro recommends that you always check the Readme text for information on known issues that could affect installation or performance, as well as a description of what's new in a particular release, system requirements, and other tips.

Other Useful Resources

Mobile Security offers a host of services through its Web site, http://www.trendmicro.com.

Internet-based tools and services include:

- Virus Map– monitor malware incidents around the world
- Virus risk assessment– the Trend Micro online malware protection assessment program for corporate networks.

About Trend Micro

Management Server, Inc. is a global leader in network anti-malware and Internet content security software and services. Founded in 1988, Trend Micro led the migration of malware protection from the desktop to the network server and the Internet gateway–gaining a reputation for vision and technological innovation along the way.

Today, Trend Micro focuses on providing customers with comprehensive security strategies to manage the impacts of risks to information, by offering centrally controlled server-based malware protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and service providers worldwide to stop malware and other malicious code from a central point, before they ever reach the desktop.

For more information, or to download evaluation copies of Trend Micro products, visit our award-winning Web site:

http://www.trendmicro.com

Index

TREND MICRO INCORPORATED
10101 North De Anza Blvd. Cupertino, CA., 95014, USA
Tel:+1(408)257-1500/1-800 228-5651   Fax:+1(408)257-2003   info@trendmicro.com

www.trendmicro.com

Item Code: TSEM95922/130402