Trend Micro Incorporated reserves the right to make changes to this document and to the service described herein without notice. Before implementing the service, please review the readme file and the latest version of the applicable user documentation.

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

Copyright © 2017 Trend Micro Incorporated, Consumer Technical Product Marketing. All rights reserved.


At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at mobile@trendmicro.com.

For support regarding Trend Micro Mobile Security for Android, go to:


DOCUMENT PROFILE:

Product Name: Trend Micro™ Mobile Security 9.0 for Android
Document Title: Trend Micro™ Mobile Security 9.0 for Android - Product Guide
Document Release Date: September 12, 2017
Team: Consumer Technical Product Marketing
# Contents

Trend Micro Mobile Security – Quick Overview ................................................................. 4  
Chapter 1: Introducing Trend Micro™ Mobile Security ..................................................... 5  
  Key Features .................................................................................................................. 6  
  System Requirements .................................................................................................... 6  
  Incompatible Software ................................................................................................. 8  
  Internet | 3G-4G Connection ......................................................................................... 8  
  Recommended Environment ......................................................................................... 8  
  Target Market ............................................................................................................... 8  
  Availability .................................................................................................................. 8  
  Contacting Trend Micro .............................................................................................. 9  
  Consumer Support Line ............................................................................................... 9  
  Email and Chat Support ............................................................................................. 9  
  Premium Services ....................................................................................................... 9  
Chapter 2: Getting Started with Trend Micro™ Mobile Security ........................................... 10  
  Download and Install Trend Micro™ Mobile Security ................................................... 10  
Chapter 3: Exploring Trend Micro™ Mobile Security .......................................................... 17  
  Overview of the Mobile Security Console ................................................................ 18  
  Security Scan ............................................................................................................... 19  
  Messenger Protection .................................................................................................. 20  
  System Tuner ............................................................................................................... 26  
  App Manager ............................................................................................................... 34  
  Network Protection ...................................................................................................... 36  
  Parental Controls ......................................................................................................... 39  
  Uninstall Protection ...................................................................................................... 44  
  Lost Device Protection ................................................................................................. 45  
  Lost Device Protection Portal ...................................................................................... 51  
  Social Network Privacy ............................................................................................... 54  
  Call Blocking ................................................................................................................ 56  
  Settings ......................................................................................................................... 58  
  Mobile Security on Your Android Tablet ................................................................... 60  
About Trend Micro .......................................................................................................... 62  


Trend Micro Mobile Security – Quick Overview

**Trend Micro™ Mobile Security for Android™** (v9.0) provides comprehensive protection for smartphones and tablets so you can enjoy your digital life safely. It safeguards against malicious apps, fraudulent websites, and identity theft, and includes performance-boosting tools. Also, it secures your data by allowing you to find, lock, or erase your device if it’s lost or stolen. Installing easily from the Google Play Store onto your Android smartphone or tablet, Trend Micro Mobile Security provides the following essential features (Red = updated or new):

**Mobile Security Console. Refreshed User Interface.** Provides easy access to all functions. (Free = F; Paid = P):

- **Security Scan.** Remove apps with security, vulnerability, or privacy issues. Stop installation of fake banking apps and install the real ones. **Pre-Installation Scan** blocks bad apps and malware on Google Play before they’re installed. (F, P)
- **Messenger Protection.** Get alerts to dangerous links in Line or WhatsApp messages. (P)
- **System Tuner.** Optimize your device’s Battery and Memory use. Just-a-Phone Mode and Smart Power Saver. **Shortcut** for quick tuning. (F, P)
- **App Manager.** Save valuable storage space by viewing Apps by usage, uninstalling rarely used and unused Apps and Setup Files. (P)
- **Network Protection.** Block malicious websites when browsing; block unsecured Wi-Fi hotspots. (P)
- **Parental Controls.** Lock Apps from kids’ use or filter inappropriate websites. Uninstall protection protects Mobile Security from unauthorized uninstallation. (P)
- **Lost Device Protection.** Using the online portal, locate a lost device, trigger an alarm, remotely lock it, or even wipe the device to protect your personal information. **New! Secret Snap** takes a photo of whoever’s found or stolen your device after a specified number of failed attempts to log into it. (P)
- **Social Network Privacy.** Fix your Facebook™ privacy settings and protect from ID or data theft. (F, P)
- **Call Blocking.** Block and disconnect annoying calls from unknown numbers. (P)
Chapter 1: Introducing Trend Micro™ Mobile Security

This chapter introduces you to Trend Micro™ Mobile Security 9.0 for Android. The topics discussed in this chapter include:

- Key Features
- System Requirements
- Incompatible Software
- Internet | 3-G-4G Connection
- Recommended Environment
- Target Market
- Availability
- Contacting Trend Micro
Key Features

All features of Trend Micro Mobile Security for Android are available during the 7-day Free Trial. When the Trial has expired, you can use it for Free, but you must buy a subscription (Paid) to re-enable the full feature set.


(Red = updated or new)

Table 1. Trend Micro Mobile Security (9.0) for Android (1 of 2)

<table>
<thead>
<tr>
<th>Android Security Features</th>
<th>Free</th>
<th>Paid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Console: Refreshed User Interface</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security Scan: Enhanced Scanning Engine - Enhanced scanning engine provides superior virus, vulnerability, and privacy protection for your device.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security Scan: Real-time Scan - Scans apps you download and install to filter out viruses and malware that can steal your information and cost you money.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security Scan: Pre-Installation Scan - Simplified Pre-Installation Scan blocks viruses and malware before they’re downloaded and installed.</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Security Scan: Updates - Unlimited updates to virus protection files.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security Scan: Cloud – Cloud scan connection ensures continuous protection.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security Scan: Fake Banking Apps - Mobile App Reputation helps you stop the installation of fake banking apps and install the real ones instead.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security Scan: Malware / Ransomware Cleaner - Removes malware and ransomware from your device</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security Scan: Privacy Scanner - Detects spyware by scanning all apps with Mobile App Reputation to identify ones that collect and potentially steal private information.</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Messenger Protection - Protects messages from bad links in LINE and WhatsApp messengers</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>System Tuner: Memory Status and Optimizer - Helps free up memory and CPU to maximize performance. Shortcut for quick tuning.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>System Tuner: Battery Optimizer - Maximizes your battery’s life.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>System Tuner: Just-a-Phone - Turns off power-draining features and apps.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>System Tuner: Auto Just-a-Phone - Turns off power-draining features and apps automatically.</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
### Table 2. Trend Micro Mobile Security (9.0) for Android (2 of 2)

<table>
<thead>
<tr>
<th>Android Security Features</th>
<th>Free</th>
<th>Paid</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System Tuner: Smart Power Saver</strong> - Intelligently manages and disables the network connection when it is not in use to maximize the battery life.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>App Manager</strong> - Saves valuable storage space by showing you Apps by usage and size, letting you uninstall rarely used and unused Apps and Setup Files</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Network Protection: Safe Surfing</strong> - Uses the Trend Micro™ Smart Protection Network™ to block malicious websites.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Network Protection: Wi-Fi Checker</strong> - Checks and notifies users of unsecured Wi-Fi Networks</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Parental Controls: App Lock</strong> - Locks Apps from use, requiring password, pattern, or PIN to open</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Parental Controls: Wi-Fi Filter</strong> - Filters inappropriate websites with age-based restrictions.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Lost Device Protection: Remote Locate / Alarm</strong> - Helps you find your devices on a Google map using GPS, cell towers, or Wi-Fi / Enables you to trigger an alarm on your device – even if it is in silent mode.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Lost Device Protection: Remote Lock / Wipe</strong> - Remotely lock your device (accessing the phone again will require that you insert your Trend Micro password or a unique unlock code). Perform a factory reset of the device from the web portal to erase all your personal data.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Lost Device Protection: Secret Snap</strong> - Takes a photo of whoever’s found or stolen your device after a specified number of failed attempts to log into it.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Lost Device Protection: SIM Card Protection</strong> - Automatically locks your device if the SIM card is removed (Accessing the phone again will require that you insert your Trend Micro password or a unique unlock code). Automatically locates your device when the following actions take place: SIM removal, SIM replacement, Phone Restart.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Lost Device Protection: Last Known Location</strong> - Automatically locates your device when the following actions take place: SIM removal, SIM replacement, Phone Restart.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Lost Device Protection: Low Power Location</strong> - Records the location of your device just before it runs out of power.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Scan Facebook: Social Networking Protection</strong> - Scan your Facebook™ privacy settings to protect you from spying and identity theft.</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Call Blocking</strong> - Filters unknown callers with whitelist and blacklist.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Uninstall Protection</strong> - Prevents unauthorized removal of the app.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Online Technical Support</strong> - Offers support provided via online forums, knowledgebase, and email.</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
System Requirements

Table 3. Trend Micro Mobile Security 9 for Android - System Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Systems</td>
<td>Android OS 4.0 and above</td>
</tr>
<tr>
<td>Device Space</td>
<td>50MB (minimum)</td>
</tr>
<tr>
<td>Memory</td>
<td>40MB-100MB Android (varies by device)</td>
</tr>
<tr>
<td>Other</td>
<td>3G/4G (LTE)</td>
</tr>
</tbody>
</table>

Incompatible Software

To identify software that you should remove from the device before installing Trend Micro Mobile Security, please refer to the following Web site:


Internet | 3G-4G Connection

Trend Micro Mobile Security uses a Wi-Fi Internet or 3G-4G connection for activating the program online, checking the expiration date, downloading updates, sending Trend Micro URL/web queries and logs to the portal, logging into the management portal, and browsing knowledge-based pages on the Trend Micro Web site.

3G-4G data connections fees are usually charged on a monthly basis, using a fixed allocation with an upper limit. If you exceed this limit, you will be charged additional fees for the amount of time connected or for the amount of data downloaded. Testers are therefore encouraged to use a Wi-Fi router-based connection to the Internet whenever possible.

Recommended Environment

This Product Guide assumes that you are using Trend Micro Mobile Security in conjunction with a PC or Mac, so you can log in to the Trend Micro Mobile Security Portal easily at http://www.trendmicro.com/LostDevice and review your Lost Device Protection settings and execute certain actions.

Target Market

Trend Micro Mobile Security is targeted to mobile users who wish to secure their Android and iOS smart phones and tablets from malicious applications, web threats to them and their family, unwanted calls and messages, and device loss.

Availability

September 12, 2017 – Google Play Store
Contacting Trend Micro

Trend Micro Incorporated
225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900
Toll-free: (888) 762-8763
www.trendmicro.com

Consumer Support Line

(800) 864-6027
Monday - Friday, 5:00AM - 8:00PM Pacific

Email and Chat Support

Paid users of Mobile Security may obtain free email, chat, and community forum support. For more information, contact eSupport at: www.trendmicro.com/support/home.

Premium Services

Trend Micro offers Premium Services for a wide variety of technical issues including installation, virus and spyware removal, PC Tune-ups, and more. For more information, visit www.trendmicro.com/support/home.
Chapter 2: Getting Started with Trend Micro™ Mobile Security

This chapter gets you started with Trend Micro™ Mobile Security. Topics discussed in this chapter include:

- Downloading and Installing Trend Micro Mobile Security
- Registering to / Creating a Trend Micro Account
- Using an Activation Code
- Buying / Activating a License
- Transferring an Existing License

Note: Trend Micro Mobile Security is included with Trend Micro Maximum Security and Premium Security. To download the bundled software, users of these editions can simply launch the Trend Micro Security Console. A “Protect Another Device” link to the Mobile Security download is available in the Console.

Download and Install Trend Micro™ Mobile Security

To download and install Trend Micro Mobile Security:

1. Open your browser on your Android device and type [www.trendmicro.com/mobilesecuritydownload](http://www.trendmicro.com/mobilessecuritydownload).
2. This takes you directly to the Google Play Store page for Trend Micro Mobile Security & Antivirus.
3. Alternately, tap the Google Play Store icon on your Android device to load it. The Google Play Store screen appears.
5. Trend Micro Mobile Security & Antivirus will appear at the top of the Apps list.


7. Tap Install. The App Permissions screen appears, indicating the access permissions Trend Micro Mobile Security & Antivirus needs on your device.


9. When installation is complete, you’re presented with a screen to Open or Uninstall the app. Tap Open. A Welcome - License Agreement screen appears.
10. The **Welcome** screen appears with the **Trend Micro License Agreement**.

11. Read the **License Agreement** by tapping the link. If you accept the terms of the agreement, tap **Accept and Continue**. A screen appears, asking you to **Help Make Mobile Security Better** by tapping **Join** to send anonymous data to Trend Micro to improve the program. Alternately, tape **Skip**.

12. A **Welcome** demo screen appears. Tap **Close** to close the demo screen.

13. A **Set Up Account** screen appears, letting you **Sign In** to a **Trend Micro Account** you already have, or to **Create an Account**.

**Option 1: If You Have An Account**

14. Tap the first option **Sign In**. The **Sign In** screen appears.
15. Enter the email address and password for your Trend Micro account and tap Sign In. You’re signed into your account and the Trial or Paid status of your install of Mobile Security is shown in the Console.

Option 2: To Create an Account


17. Enter your preferred email address, your first and last name, choose your location from the drop-down menu, and tap Next.

18. Confirm your chosen email address, then enter a password and confirm it for your new Trend Micro Account.

19. If you wish, check Receive the latest news and offers from Trend Micro, and tap Done.

20. Trend Micro Mobile Security is activated and registered to your account and the Console opens. The activation can be as a 7-day Trial subscription, or an expired or new subscription, showing the past or future expiration date. You have several options to upgrade Trial or Expired subscriptions:

   Option 1: If you already have an Activation Code, you may apply it to this device.

   Option 2: You may Purchase a subscription.

   Option 3: You may Transfer another license you own to this device.
To apply the Options to Trial or Expired Subscriptions:

1. Tap the **Buy / Activate** link in the **Console**. The **Buy / Activate** screen appears.

   **Option 1 - Activate**

2. Tap **Use an Activation Code**.

3. In the screen that appears, enter the **Activation Code** you received in your confirmation mail or in your retail box and tap **OK**. Your subscription is activated.

   **Option 2 - Purchase**

4. Tap a **Purchase** option in the **Buy / Activate** screen. The subscription popup appears.

5. Tap **Subscribe**. The card you registered with your Google Account will be charged and your subscription will be activated.
Option 3 - Transfer:

6. With the Console visible, tap the Options menu on your device, then the Settings menu in the Options popup. The Settings screen appears.

7. In the Settings screen, tap Transfer a subscription to this device. The Transfer Subscription screen appears.

8. Scroll down to locate a viable subscription; e.g., Not Yet Installed or one that is already installed, and tap it.

9. A popup appears, asking if you wish to Switch to Another Subscription.

10. Tap OK to make the switch. If it’s a new installation, the subscription will immediately be activated on this device. If it’s already activated on another device, it will be deactivated on that device and transferred to this one.
11. The **Console** will indicate **Your subscription has been updated** and your new expiration date will be applied to the installation.

12. You’re now ready to use **Trend Micro Mobile Security** on your Android device! See the sections following for instructions.

![Figure 25. Updated Subscription](image)
Chapter 3: Exploring Trend Micro™ Mobile Security

This chapter provides an overview of Trend Micro Mobile Security (TMMS). Topics discussed in this chapter include:

- Overview of the Mobile Security Console
- Security Scan (Includes Pre-Installation Scan)
- Messenger Protection
- System Tuner
- App Manager
- Network Protection
- Parental Controls
- Lost Device Protection
- Secret Snap
- Social Network Privacy
- Call Blocking
- Settings
- Mobile Security on your Android Tablet
Overview of the Mobile Security Console

Once installed, Trend Micro™ Mobile Security (TMMS) appears in your Applications list on your Android mobile device and a shortcut appears on the desktop of your device.

To use the Mobile Security Console:

1. Tap the Trend Micro Mobile Security icon on your mobile device and the Mobile Security Console appears.

2. Simply tap a button or panel to access the Console functions. Tap, hold and scroll to see panels lower down in the Console function list.

3. For example, tap the Scan wheel to do a Device Scan.

4. Or tap the [X] things to fix in the Status Banner; then tap the alert panel to remove a threat. The Security Scan screen appears.

5. In the Security Scan screen, tap the Apps: Removal Recommended panel to view apps you may want to Remove from device or add to the Trusted Apps list.

6. Tap a panel in the scrolling Console, e.g., Messenger Protection (Figure 26), to execute the function or configure its settings. More details below.
Security Scan

To use the Security Scan:

1. Tap the Security Scan panel in the Console. The Security Scan settings screen appears, with the Settings tab active by default.

2. Tap Scan Now to conduct a security scan. The Security Scan performs a combination security, vulnerability, and privacy scan and returns the result.

3. In the example shown, “Citibank” has been detected as a fake banking app, (present on the device before Mobile Security was installed.) Apps are also recommended for removal (or to trust).

4. Tap Uninstall to uninstall the fake app. A Details screen defines the security threats.

5. Tap Uninstall again. A popup will ask if you want to uninstall the app; tap Uninstall once more to uninstall it.
6. Back in the Security Scan > Settings screen, tap the Settings options to configure them. These include:

**Protection Strength.** Choose the level for alerts:

- **Low.** Receive alerts only for apps confirmed as fraudulent or dangerous.
- **Normal.** Receive alerts for regular daily use, without notifications about minor risks.
- **High.** Receive alerts for apps that show any signs of fraud or danger.

**Real-Time Scan.** Option is checked by default and provides a real-time scan of all downloaded apps.

**Pre-Installation Scan.** Disabled by default. Blocks malware from Google Play before it’s installed. To enable, see the following section.

**Scan Memory Card.** This option, unchecked by default, checks the memory card for security threats.

*Scan Option. Scan only apps (default) or Scan all files.*

**Trusted Apps.** Tap Trusted Apps > App then Remove from the Trusted List to remove an app from the list.
To enable the Pre-installation Scan:

1. Tap the Pre-installation Scan panel in the Security Scan > Settings screen. The Pre-installation Scan toggle screen appears.

2. Note that the Pre-installation Scan requires the Accessibility permission for Mobile Security to be turned on.

3. Tap the Pre-installation Scan toggle from Off to On. The demo screen for turning on Accessibility appears.

4. Tap Turn On Now. The Accessibility screen appears.

5. Scroll down the screen and tap the panel for Mobile Security. The screen to enable Mobile Security accessibility appears.
6. Note that Accessibility Permission is needed for SafeSurfing, Messenger Protection, the Pre-installation Scan and App Freeze.

7. Tap the toggle from Off to On.

8. If your device has Secure Startup turned on in Android, a popup will appear to turn it off. Mobile Security wants permission to monitor your actions and retrieve window content.

9. Tap OK. Your PIN window appears.

10. Enter your PIN and tap Done.

11. Mobile Security’s Accessibility permission is turned on.

12. Tap the back-arrow. The Pre-Installation Scan toggle is now On.
13. Now all apps downloaded from Google Play will be scanned for malware before they’re installed.

14. Test the Pre-Installation Scan by downloading an Antivirus Test app from Google Play.

15. Enter “Antivirus Test” into the Google Play Search field.

16. When the search results appear, pick an antivirus test for download.

17. For example, tap Test your antivirus.

18. Mobile Security’s Pre-Installation Scan presents a popup saying Test your antivirus is dangerous.

19. Do not install the app, as it presents dangers to your device.

20. Use the back-arrow on your device to back out of the Install screen.
Updates and History:

1. Tap the Update tab in the Virus Scanner screen. The Update options appear.

2. Tap the Update button to manually update the pattern file. Mobile Security updates. If Automatic Scan is checked, a scan is conducted after an update.

3. Variously check Auto Update, Auto Updates require Wi-Fi.

4. Tap Auto Update Schedule and a popup appears, letting you choose your Update Interval: Daily, Weekly, or Monthly.

5. Tap the History tab, then the Security Scan or Updates panels to obtain a history of threats found or updates conducted.

6. Tap the Trashcan in the individual History panels if you wish to delete the history.
Messenger Protection

Mobile Security’s **Messenger Protection** alerts you to dangerous links when you use Line and/or WhatsApp on your mobile device. To use the function, you need to first install Line or WhatsApp and enable the **Accessibility** option for Mobile Security in your phone settings. (See previous section.) In this example, Line has also been previously installed.

To use Messenger Protection:

1. Tap **Messenger Protection** in the Mobile Security Console. The **Messenger Protection** screen appears, with the function turned **Off** by default.

2. Tap the toggle from **Off** to **On**. You’re now protected from dangerous links in **LINE** and **WhatsApp**.

3. Tap **Settings** to set your **Protection Level**.
   - **Low**. Blocks only sites confirmed as fraudulent or dangerous.
   - **Normal**. Provides balanced protection without blocking minor risks.
   - **High**. Blocks sites showing any signs of fraud or malicious software.

   **Note**: The level you select here will also be used for **SafeSurfing**.

Figure 5. Messenger Protection

Figure 5. Messenger Protection > Applications

Figure 5. Messenger Protection > Settings
System Tuner

Mobile Security’s **System Tuner** lets you optimize the battery and memory settings on your device, as well as to clean up your clipboard data, web browser and Google Play search histories. Battery optimization tools include **Just-a-Phone Mode**, to manually or automatically turn off many settings to save battery power when it’s especially low; and the **Smart Power Saver**, to automatically change Wi-Fi, 3G/4G, and Bluetooth connections upon idle to also save power.

To use System Tuner:

1. Tap **System Tuner** in the Mobile Security Console. The System Tuner screen appears.

2. Tap **Add a shortcut to homescreen** to add a shortcut for future quick optimization of your phone, saving memory and battery.

3. Note the popup banner at the top telling you that Mobile Security needs more permissions before you can use all of the System Tuner features.

4. Tap the popup. The **Allow Permissions** popup appears.
5. Depending on your configuration, different permission options will be highlighted as needed.

6. In this example, tap Apps with usage access. A demo screen appears, suggesting you tap Turn On Now.

7. When the Usage Data Access screen appears, tap Mobile Security to turn on usage data access for the app. The Usage Data Access screen for Mobile Security appears.

8. Tap the toggle Allow usage tracking from Off to On.

9. When you’re done, tap the back arrow to return to the Allow Permissions screen.
10. Tap **Phone permission**. The demo screen appears, asking you to tap **Turn On Now**.

**Note:** The permissions screen can be accessed through your phone **Settings > Apps > App manager > Mobile Security > App Settings > Permissions**.

11. Tap **Turn on Now**. The **App Info** screen for Mobile Security appears.

12. Tap **Permissions** for Mobile Security. The **App Permissions** screen appears.

13. Toggle on each of the **App Permissions** in turn.
14. When you’ve finished turning on the permissions you’ve chosen, tap your device back-arrow to return to the **Permissions** popup, then tap **OK** to complete the process. **System Tuner** is now set up to maximally optimize your system.

15. To optimize your system, do one of two things:
   - Tap **Optimize** for a quick optimization.
   - Tap **Apps in Use**, check those apps you wish to keep running, then tap **Optimize**.

17. When it’s done, you’re presented with a **Device Optimized** screen that calculates the extra memory and battery time saved.

18. To further optimize your system by doing a **Force Stop** on selected apps, tap **Open App Freeze**. The **App Freeze** screen opens.

19. Check apps you want to freeze, then tap **Stop Apps**.

20. Selected apps will be force stopped, optimizing memory and battery. Reopen the app to restart all of its functions at any time.

21. Note that you cannot multi-task while this operation is in progress; i.e., when Mobile Security is freezing a number of apps. Tap **Cancel** to back out, if so desired.

22. When the **App Freeze** is complete, tap **Close** to close the screen.
To use Just-a-Phone Mode:

1. Tap the Just-a-Phone Mode toggle to the right to turn it on. The Ready for Just-a-Phone Mode screen appears.

2. Tap Turn On to enable Just-a-Phone Mode. The Just-a-Phone Mode is enabled according to the default Just-a-Phone Options.

3. To adjust those options, tap Auto Just-a-Phone. The Auto Just-a-Phone screen appears.

4. Tap Auto Activate and Auto Activate Threshold to enable those auto-activate functions.

5. Tap Set Schedule to adjust the schedule Start and Stop times, and tap OK.
6. Tap **Set Threshold** to set the battery power threshold at which **Auto Just-a-Phone** is activated.

7. By default, the **Just-a-Phone Options** section shows all four items checked:
   - Switch off 3G/4G
   - Switch off Wi-Fi
   - Switch off Bluetooth
   - Stop any running apps

8. Uncheck any options you wish to keep active during **Just-a-Phone**, whether on-demand or auto-activated, and tap **Save**.

---

To enable **Smart Power Saver**:

1. Tap the **Smart Power Saver** panel to access its settings.

2. Check **Turn on Smart Power Saver** to turn it on.

3. The option to maintain your 3G/4G connection, so you can receive instant messages and email, is checked by default. Uncheck it if you wish.

4. Check/uncheck the various settings in **Smart Standby** and **Smart Wi-Fi** to enable the changes to W-Fi, 3G/4G, and Bluetooth to save power.
5. For **Smart Standby**, set how long after the screen darkens to switch-off 3G/4G and Bluetooth.

6. Also for **Smart Standby**, set at what intervals 3G/4G will switch on again to make a connection for email/text messages.

7. For **Smart Wi-Fi**, set the interval to switch off Wi-Fi.

8. Again, for **Smart Wi-Fi**, set the interval when it will switch on again to make a connection.
App Manager

App Manager lets you remove unwanted files and apps, including setup files, which can take up unnecessary memory and space on your device.

To use App Manager:

1. Tap **App Manager** to manage your apps. A demo screen appears, showing you how to change your sorting options.

2. Tap **Ok** to close the demo screen. The App Manager **Uninstall** tab displays.

3. Using the **Sort** menu in the upper right, sort by **Size**, **Date**, **Name**, or **Last used**, if you wish.

4. Scroll down to view apps you might want to uninstall; or tap **Pre-installed apps** and check the checkbox for an app to uninstall.

5. Tap **Uninstall**. A screen or popup appears, asking “Do you want to uninstall this app?”

6. Tap **OK** to uninstall the app(s). The app is uninstalled.

7. Tap **Setup Files** to delete APK files. Lists of **Installed** and **Not Installed** APK files appear.

8. Check those you wish to delete, then tap **Delete** to delete the setup files. The files are deleted.
Network Protection

Network Protection enables two types of protection on your mobile device: SafeSurfing provides web threat protection when you’re surfing the net; and Wi-Fi Checker checks for unsecured Wi-Fi hotspots and notifies you when your mobile device provides an offer to connect to it. You can accept or reject the connection and add the Wi-Fi network to your list of Trusted or Blocked Wi-Fi hotspots.

To use Network Protection:


2. SafeSurfing and the Wi-Fi Checker are turned on by default and the SafeSurfing Protection Level tab is pre-selected.

3. Use the selection slider to set the strength of your SafeSurfing Protection. The level you set will also be applied to Messenger Protection.

   Low. Blocks sites confirmed as fraudulent or dangerous.

   Normal. Provides balanced protection without blocking minor risks.

   High. Blocks sites showing any signs of fraud or malicious software.
4. When you browse to a dangerous website in your browser, Mobile Security blocks it and gives you a Dangerous Page message, as shown in this test site.

5. To add a URL to the SafeSurfing Blocked or Approved Lists, tap the name of the respective list from the settings page or the drop-down menu; e.g., Blocked List. The Add screen appears.

6. Tap Add. A popup appears. Type the name the item and the URL and tap Save. The URL is added to the Blocked or Approved List.
7. If it’s in the Blocked List, **SafeSurfing** will block it if you try to go to the website.

8. Similarly, the **Wi-Fi Checker** will notify you with a popup if you if your mobile device is connected or tries to connect to an unsecured Wi-Fi network.

9. Tap **Settings** to forget the unsecured Wi-Fi network in the future; or tap **Trust Wi-Fi** to add it to the **Trusted Wi-Fi List**.

10. To view trusted Wi-Fi hotspots, tap the **Wi-Fi Checker** tab. The **Trusted Wi-Fi List** appears.

11. Tap the **Trusted Wi-Fi List** to view the list; then if you wish, select any Wi-Fi network and tap **Trashcan** to remove it from the list.
12. Tap the History tab to view your SafeSurfing History; then tap the SafeSurfing panel to show the history of all sites blocked by SafeSurfing.

13. Once you see the list, tap-hold the item(s), then tap the Trashcan to delete all selected SafeSurfing events; or tap a specific event, then the Trashcan to delete the history.
Parental Controls

Mobile Security’s Parental Controls lets you lock apps and block inappropriate websites to help protect your kids.

To use Parental Controls:

1. Tap Parental Controls to access its settings. The Password screen appears.

2. The first time you enter Parental Controls or Lost Device Protection settings, the Unlock screen defaults to requiring your Trend Micro Account Password.

3. Enter your Trend Micro Account Password to unlock the Parental Control settings screens. The App Lock screen appears, with the toggle turned Off.

4. If you wish, tap the Lock Settings icon in the upper right corner of the screen to change your Password to a Pattern or a PIN, which may be easier to remember. The Lock Settings screen appears.

5. Tap Pattern if you wish to create a Pattern Lock.
6. Draw a **Pattern** and when prompted, draw it again to confirm it and tap **OK**.

**NOTE:** Use a less obvious, more complicated pattern than the one shown, to increase your protection.

Your password changes to the unlock pattern you’ve specified.

7. Similarly, tap **PIN** if you wish to use a 4-digit PIN. The **Set PIN** screen appears.

8. Type in a 4-digit PIN, then enter it again to confirm it, and tap **OK**. Your PIN is created successfully.

9. You’ll use the **Pattern** or **PIN** when you want to make non-critical changes to your Mobile Security settings. For changes Trend Micro deems critical, you’ll still need your **Trend Micro Account Password**.
To configure App Lock:

1. Tap the **App Lock** toggle to turn the function **On**. A demo screen appears; tap **OK** to close it. **App Lock** is turned on and your device **Settings** app is locked by default.

2. Tap **Apps** you wish to lock. The apps you add to the **App Lock** list will prompt you to enter the unlock key when you open them for use.

3. Note the **Lock** icon below the **App Lock On/Off** toggle. When selected, those apps you’ve locked appear at the top, sorted alphabetically. Tap the lock **Off** to return to a basic alphabetical sort ordered by all the apps on your device.
To configure Website Filter:

1. Tap the Website Filter toggle to turn it On. A demo screen appears; tap Close to close it. The Protection Level is Teen by default.

2. Set your Protection Level by tapping the selection button for the preferred level:
   - **Child.** Provides filtering for children 9 or younger.
   - **Pre-teen.** Provides filtering for children between 10 and 13.
   - **Teen.** Provides filtering for young adults between 14 and 18.

3. Tap Blocked List to add a website you wish to block. The Blocked List appears.

4. Tap Add. The Lock screen appears.

5. Enter your Trend Micro Account Password and tap OK. The Add popup appears.

6. Type a Name for the website block, then enter the actual URL for the Website and tap Save. The website is added to the Blocked List.

7. You can now test for web threats and filtered websites. (The settings apply to your Native Android browser and Chrome only.)
8. Enter a URL into your browser’s search field that you know or suspect is dangerous.

9. **OR:** Enter a URL that is inappropriate for the Protection Level you’ve designated for your children.

10. **OR:** Enter a URL you’ve put on the Blocked List.

11. In each case, Mobile Security will block the website and display a warning.

12. Tap Approved List to add a website to the Approved List; then repeat the instructions given above for adding the URL.

13. Tap History to view a history of blocked webpages.
Uninstall Protection

To enable Uninstall Protection:

1. Back in the main Parental Controls screen, toggle Uninstall Protection On to protect Mobile Security from unauthorized uninstallation and to keep your kids protected with Parental Controls. A screen appears, explaining how to use Uninstall Protection and to turn it off, if you wish to uninstall Mobile Security.

2. Tap Ok. A screen appears for you to Activate Phone Administrator.

3. Review the operations allowed when you activate the phone administrator, then tap Activate. A screen appears for you to provide your password, PIN, or pattern.

4. In this example, Provide your PIN. A popup screen appears, indicating Device Administrator Activated.
5. Tap OK to close the popup. **Uninstall Protection** is on.

---

**Lost Device Protection**

To enable Lost Device Protection:

1. Back in the main **Console**, tap **Lost Device Protection**. The login screen appears.

2. Enter your **Password**, **Pattern**, or **PIN**. The **Lost Device Protection** screen appears, with the **Find My Android** tab selected by default and three options displayed:

   **SIM Card Lock.** Lock this device if the SIM card is changed or removed.

   **Device Name.** Click the **Edit** icon to change the device name.

   **Remote Lock.** Display this message after locking the device.
Remote Wipe. Allows you to do a partial or full wipe of your device remotely.

3. Tap SIM Card Lock if you wish to lock your device when the SIM card is changed or removed. A Password Required screen appears.

4. Enter your Trend Micro Account password and tap OK. SIM Card Lock is enabled.

5. Tap the Device Name panel edit pencil to change your device’s name, make your changes in the edit window, and tap Save.

6. Tap the Remote Lock panel edit pencil to display the message after locking the device, make your changes in the Edit Message screen, and tap Save. Your message changes are saved.

7. Tap the Remote Wipe tab to access the feature. The Remote Wipe screen appears, with Full Remote Wipe selected. This lets you delete all content from the Lost Device Protection website in the event your device is lost or stolen.
Note: Full Remote Wipe is selected if you’ve turned on Uninstall Protection, as given in the previous section. Otherwise, Partial Remote Wipe will be selected.

8. If you wish, tap Partial Remote Wipe to change to the partial wipe. The Password Required screen appears.

9. Enter your password and tap OK.

10. The option switches to Partial Remote Wipe and turns off the Uninstall Protection of Mobile Security. Turning Uninstall Protection back on will revert the wipe function to Full Remote Wipe.

11. Manage your protection in the Lost Device Protection Portal. See below for details.
To Use Secret Snap:

1. Tap Secret Snap to set your device to take a photo after a number of incorrect attempts to unlock your device. The Secret Snap editor appears.

2. Tap the toggle to turn Secret Snap from Off to On. The Activate Phone Administrator screen appears.

3. Tap Activate to activate the administrator. The Password/PIN/Pattern screen appears.

4. In this example, provide your PIN.
5. **Secret Snap** is turned on.

6. Tap the panel to set the number of incorrect attempts to access your device before a photo is taken.

7. Choose 3, 5, or 7 attempts and tap **Save**.

8. Tap the **Notification Email** pencil to change the email address where the photo notification will be sent, then tap **Save**. You’ll be able to view the photos taken in this email.

9. After you’ve recovered your phone, you can review any photos stored on your device by tapping the **Secret Snap Photos** panel. The photo list appears.
10. Tap a photo to view it, or tap the Trashcan to delete it.

11. As mentioned, you can also view the photo in the notification email sent to you by Mobile Security. This can be used with the Lost Device Protection Portal’s location feature to help locate the person who has found or stolen your device.

12. Click the link To Locate Your Device using the Lost Device Protection Portal.

13. To obtain assistance, visit www.trendmicro.com/mobilehelp.
Lost Device Protection Portal

To access the Lost Device Protection Portal:

1. Launch your browser on your PC and type https://mobilesecurity.trendmicro.com/ into the search field, and hit Enter. The Lost Device Protection Portal webpage appears.

2. Tap Find Now or Sign in to sign into your Trend Micro account. The Sign In page appears.

3. Type the email address and password you used to create your Trend Micro account and click Sign in. The Lost Device Protection Portal appears.

4. You’re presented with a Device List on the left, a Bing Map on the right with a GPS/Bing estimate of your location, and a toolbox to perform various operations regarding your lost or stolen device.
5. In the **Device List**, click **Hide** to hide any device in the main list. Click the down-arrow to see **Hidden Devices**.

6. Click **Share** to share the device’s location with a trusted friend.

7. Click **Alarm** to sound a one-minute alarm on your missing mobile device, even if it has been set to silent mode.

8. Click **Locate** to locate the phone on the map.

9. Click **Reset** to force stop apps and to **Reset the Lock Screen Password**.

10. Click **Lock** to stop anyone from using your missing mobile device. When you recover your device, click **Unlock** to unlock it, then use the **Unlock Key** provided or your Trend Micro password to complete the unlock.

11. Click **Device Detail** (below the device icon in the list) to view the unlock code that can be entered into the device interface to unlock the device instead of the master account password. This key can also be emailed to you at your account email address by tapping **Email Yourself an Unlock Key** on the device once it’s found.

12. Click **Wipe** to permanently delete all content.

---

**Figure 146. Lost Device Protection Options**

**Figure 147. Unlock**

**Figure 148. Device Unlock**
the data stored on your missing mobile device.

13. A warning appears. If you wish to wipe your device, click **OK**.

**Warning**: Using this feature will perform a factory reset of your device. For testing or review purposes, please ensure you are using a test device or have a complete backup of your information. Once reset, TMMS will be removed from the device and the location feature will no longer function.
Social Network Privacy

Trend Micro Mobile Security also includes Social Network Privacy scanner to help edit your Facebook Privacy Settings.

To access Facebook Privacy Scanner:


2. Tap Sign into Facebook to check your privacy settings. The Facebook Login screen appears.

3. Enter the email address and password you use to sign into Facebook and tap Log In. Facebook Privacy Scanner checks your privacy settings.

4. When it’s done checking, it presents you with the analysis.
5. Tap each item in the list to reset it to the recommended setting. A popup appears, letting you make the change.

6. Check the recommended Privacy Setting. In this case, change the setting from Friends of friends to just Friends, to increase your privacy, and tap OK.

7. Privacy Scanner makes the change, saying Great! Issue Fixed.

8. Since Facebook periodically changes its privacy policies or adds new features to the social network, you should periodically rescan your privacy settings to ensure your privacy.
Call Blocking

To block unwanted calls:

1. Back in the main TMMS Console screen, tap Call Blocking. The Call Blocking screen displays, with the Call tab selected by default and Call Blocking enabled. Tap the slider to the left to disable the function.

2. Tap Filtering Method to change the filtering option in the popup:
   - Stop only blocked callers
   - Allow only approved callers
   - Allow approved and anonymous callers

3. Tap Action to change the action to be performed in the popup.
   - Reject call
   - Silence device
   - Reject call + send reply

4. Tap Reject call + send reply and you’re given three preset options for Automatic Reply.
5. Check **Block Annoying Calls** from unknown numbers to disconnect them within three seconds.

6. Tap the **Blocked / Approved** lists to add a number to either list. The **List** tool at the top of the screen also gives access to the lists.

7. Tap the **Plus (+)** tool to add the number; you can also use the drop-down to switch easily between lists.

8. Tap **History > Blocked Call History** to review your **Blocked Call History**.
Settings

Trend Micro Mobile Security provides system settings for app management.

1. Tap **Mobile Security** on your device to open the **Console**.
2. Tap the **Settings** menu on your device to open the popup.
3. Here, you have access to various options.
   - **Settings**: Access various system-level settings.
   - **Renew / Activate**: Renew or activate a subscription.
   - **Help**: Get Online Help with Mobile Security.

4. Tap **Settings** to access system-level options. The **Settings** screen appears, with the list of options available. Scroll down to view the options.
   - **Trend Micro Account**: Account you’re registered to.
   - **Expiration Date**: Date your subscription expires.
   - **Serial Number**: 20-character serial number
   - **Renew / Activate**: Purchase/renew or activate a subscription.
   - **Sign Out**: Disconnect your Trend Micro account.

   **Check your Trend Micro Account**: Manage your account and subscriptions.

   **Set up alternate email addresses**: Send from an unlock key from the lock screen to your Trend Micro account and the email address you set up here.

   **Display the app icon on the status bar**: Check here to show Mobile Security on the status bar.

**Share**: Send friends or associates a recommendation to use Trend Micro Mobile Security.

**Send Feedback**: Provide a rating and review on Google Play and send feedback to Trend Micro.

**Figure 164. Settings Popup Menu (Device)**

**Figure 165. Settings (1)**
Settings (continued)

**Uninstall.** Uninstall Mobile Security with your Trend Micro Account password when **Uninstall Protection** is turned on.

**Low Power Alert.** Send a notification when the battery is less than 50%.

**Low Memory Alert.** Send a notification when the memory usage is over 80%.

**About.** Product details and version number.

**Help.** Access Online Help.

**Collect logs.** Collect logs to send to Trend Micro.

**Log history.** Logs sent to Trend Micro.

**Help make Mobile Security better.** Anonymously share device information with Trend Micro.

Figure 166. Settings (2)

Figure 167. Settings (3)
Mobile Security on Your Android Tablet

Trend Micro Mobile Security works much the same way on your Android tablet as it does on
your Android smartphone, minus Call Blocking, which is a specific function for smartphones.

Whether you’re holding your tablet vertically or horizontally, the Console displays the same
functions, it just distributes them differently.

Figure 168. Mobile Security on Tablet (Vertical View)
Figure 169. Mobile Security on Tablet (Horizontal View)
About Trend Micro

Trend Micro, a global leader in security software and solutions, strives to make the world safe for exchanging digital information. For the past 25+ years, its employees have been inspired to protect individuals, families, businesses and governments as they look to harness the potential of emerging technologies and new ways of sharing information.

In today’s organizations, information has become the most strategic asset; embodying competitive advantage and powering operational excellence. With the explosion of mobile, social and cloud technologies, protecting this information has become more challenging than ever. Organizations need smart protection of information, with technology that is simple to deploy and manage, and security that fits an evolving ecosystem. Trend Micro solutions enable a smart protection strategy for organizations. Smart. Simple. Security that fits.

Trend Micro provides layered content security for mobile devices, endpoints, gateways, servers and the cloud. Leveraging these solutions, organizations can protect their end users, their evolving data center and cloud resources, and their information threatened by sophisticated targeted attacks.

All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For additional information, visit www.trendmicro.com.