# Contents

1 About Sophos Mobile Security ................................................................. 3  
2 Dashboard .................................................................................................. 4  
3 Scanner ....................................................................................................... 5  
4 Loss & Theft ............................................................................................. 8  
5 Privacy Advisor ........................................................................................ 12  
6 Security Advisor ...................................................................................... 14  
7 Log ............................................................................................................. 15  
8 Logging and tracing .................................................................................. 16  
9 Legal notices ............................................................................................ 17
1 About Sophos Mobile Security

Sophos Mobile Security is an app for Android phones and tablets that protects you from apps with malicious behaviour and secures your data in case the device is stolen or lost. It assists you in detecting apps with critical permissions and in configuring the security relevant settings of your device.

The Sophos Mobile Security app is available from the Google Play store for free.

It works on all devices with Android version 2.2 or higher.

1.1 Installation and update

You can install the Sophos Mobile Security app from Google Play. Update works via the usual mechanism for Android devices.

Uninstallation

Sophos Mobile Security needs to be device administrator to perform actions like locate or lock. To be able to uninstall Sophos Mobile Security, you have to deactivate the device administrator capability of Sophos Mobile Security.

You can do so in the Android Settings. Go to PERSONAL > Security > DEVICE ADMINISTRATION > Device administrators and deactivate the checkbox for Sophos Security.

Note: The path to a setting may vary depending on the Android version and/or the device you are using.

1.2 Android versions

The description in this manual refers to Android 4.0. As Sophos Mobile Security supports all Android versions starting with 2.2, the look and feel of the app on your device may be different.

For differences between Android versions, see http://developer.android.com/design/patterns/compatibility.html.
2 Dashboard

To start the app, tap the Security icon on the Apps screen of your Android device.

From the dashboard, you can access the features of Sophos Mobile Security:

- **Scanner**
  Checks and reports any malicious apps installed on the device.

- **Loss & Theft**
  Allows to locate and lock devices via text messages.

- **Privacy Advisor**
  Provides information about installed apps and the permissions they request.

- **Security Advisor**
  Assists you in configuring the security settings of your device.
3 Scanner

Sophos Mobile Security checks and reports any malicious apps installed on the device. Scanning the device for malware uses the Sophos cloud infrastructure. Sophos Mobile Security checks and reports any malicious app installed on the device. The scan uses an online cloud lookup to verify against the latest data in the Sophos cloud. This data is constantly updated by SophosLabs who analyze Android malware 24 hours a day. Additionally, local data comes with the app to perform checks if no online connection is available.

3.1 Configure Scanner

1. Tap the Settings icon in the upper right-hand corner of the Scanner view.

   Note: Depending on the Android version of your device the icon may not be shown. If you press the menu button on such devices, a menu with the Settings command is displayed. For further information, see Android versions (section 1.2).

2. In the Malware scanner settings view you can define the behavior of the scanner.

   ■ **Scan system apps**

      System apps are not scanned by default as they are protected by the Android OS and cannot be removed by the user. However, you can activate scanning of system apps here.

   ■ **Scan SD card, USB, ...**

      If you activate the Scan SD card, USB, ... option, Sophos Mobile Security will scan all files on SD cards, USB and other external storage devices in addition to per default scanning of all installed apps on the device.

   ■ **Detect PUAs**

      Potentially Unwanted Applications (PUAs) are apps that, while not malicious, are generally considered unsuitable for business networks. The major PUA classifications are Adware, Dialer, System monitor, Remote administration tools and Hacking tools. However, certain apps that can fall into the PUA category might be considered useful by some users.

      If you activate the Detect PUAs option, Sophos Mobile Security will detect PUAs during scans and notify the user accordingly.

   ■ **On install scan**

      Sophos Mobile Security scans apps during installation on the Android device by default. You can deactivate this behavior by deactivating On install scan.

3. Select the scans you want Sophos Mobile Security to perform.
4. Tap **Cloud scan mode** to define when Sophos Mobile Security should scan for the latest malware information.

Select one of the following options to define when the app should use a cloud lookup:

- **Always**
- **Not while roaming**
- **Wi-Fi only**

With this setting you can control the data traffic of the app. If you set **Cloud scan mode** to **Wi-Fi only**, the cloud lookup will only be performed when the device has a Wi-Fi connection. If you set **Cloud scan mode** to **Not while roaming**, a cloud lookup will never be performed while the device is roaming in a foreign network.

5. Select the scan mode.

### 3.1.1 Configure a scheduled scan

You can configure a scan schedule for Sophos Mobile Security. The app scans your device in the background based on the schedule defined. You are only notified when the scheduled scan finds malicious apps. For every scheduled scan performed, a log entry is created in the app log.

To configure a scheduled scan:

1. Go to the **Malware scanner settings** view.
2. Activate/deactivate the scheduled scan functionality with the **Scheduled scan** option. When activated, the time of execution for the next scheduled scan is displayed.
3. Adjust the scan interval with the **Scheduled scan interval** option.

### 3.2 Scan the device

1. On the apps dashboard, tap **Scanner**.
2. In the **Scanner** view, tap **Start**.

   The scan is performed according to the settings you selected on the **Malware scanner settings** view.

3. If malware is found, the malicious or suspicious app is displayed in the **Threats** section of the view.
4. Tap the app to display details.

In the **Object details** view you can uninstall the malware app by tapping **Uninstall** or add it to a list of ignored apps.
3.3 Ignored apps

If you decide to trust apps, although they have been identified as malware, you can mark them as ignored. In subsequent scans, these apps will not be shown as threats.

To add an app to the list of ignored apps, tap **Ignore** in the **Object details** view.

**Clear the list of ignored apps**

To display all apps that you marked as ignored again as a result of a scan, you can clear the list of ignored apps.

To do so go to the **Malware scanner settings** view and tap **Reset ignored apps**.

All apps will be scanned again.
4 Loss & Theft

With Loss & Theft you can locate and lock your device, for example if you lost it. This is done by sending a command text message from a previously registered phone number. The command text must have a specific format and has to include a defined password.

4.1 Configure Loss & Theft

Before you can use Loss & Theft, you have to configure the required Android settings and provide Sophos Mobile Security with some information. A wizard guides you through configuration.

1. On the app dashboard, tap Loss & Theft.

The Overview of the wizard appears where all the settings that must be configured to activate the Loss & Theft functionality are listed. Settings that are already configured are marked with a green checkmark icon.

2. Swipe to the left or tap on an item in the Overview to directly switch to the corresponding configuration wizard page.

3. Swipe left in the Overview to go to the Feature selection view. To activate or deactivate specific Lost & Theft sub-features, select or deselect the checkboxes.

4. Swipe to the left.

The Device administrator view of the wizard is displayed.

To enable Loss & Theft, Sophos Mobile Security must be device administrator.

5. Tap Activate to activate the device administrator capability.

6. In the Android Activate device administrator view, tap Activate.

Sophos Mobile Security is now device administrator and the Device administrator view of the wizard is displayed again.

7. Swipe to the left.

The Lock screen view appears.

To enable the Loss & Theft feature, the Android screen lock has to be enabled by defining a password or pattern to unlock the screen.

8. Tap on Configure to enable the Android screen lock.

In the Android Unlock selection view, select a method and configure it.
9. Swipe left.

The **Location services** view is displayed.

Sophos Mobile Security uses location services, for example GPS, to retrieve the location of a device.

10. Tap **Configure** to display the Android **Location services** view.

In the Android **Location services** view select your preferred service or services and go back to the wizard’s **Location services** view.

11. Swipe left.

The **Text message password** view is displayed.

You have to define a secret password to ensure that only you can remotely locate and lock your device.

12. Tap **Configure**, enter a password (at least 4 alphanumeric characters), confirm it and tap **Save**.

13. Swipe left.

The **Phone numbers** view is displayed.

You can define up to 5 phone numbers which you can use to locate and lock this device remotely. Sending an appropriate text message from these phone numbers will locate or lock the device immediately.

14. Enter the phone number without spaces and with country and area code, or select a number from your contacts. Enter at least one number.

Only the numbers you add here can be used to send a text message that locates or locks the device.

**Loss & Theft** is now configured and you can use it to locate or lock your device in case you lost it or it has been stolen.

### 4.2 Play alarm tone remotely

To play an alarm tone at maximum volume for one minute, even if the device is muted, you have to send a specific text message from one of the numbers you entered in the **Phone numbers** view in the **Loss & Theft** configuration.

1. Prepare a text message from one of the numbers you specified in the **Loss & Theft** configuration.

   The text message to play an alarm tone is: `alarm <Text message password>`

   `<Text message password>` is the password you defined in the **Text message password** view of the **Loss & Theft** configuration.

   For example: `alarm MyDevice996`

2. Send the text message to the device to play an alarm tone.
The device receives the text message and an alarm tone is played for one minute at maximum level.

### 4.3 Locate remotely

To locate a lost or stolen device, you have to send a specific text message from one of the numbers you entered in the **Phone numbers** view in the **Loss & Theft** configuration to the device to be located.

1. Prepare a text message from one of the numbers you specified in the **Loss & Theft** configuration.
   
   The text message to locate a device is:
   
   \[ \text{locate} \ <\text{Text message password}> \]
   
   For example: `locate MyDevice996`

   `<Text message password>` is the password you defined in the **Text message password** view of the **Loss & Theft** configuration.

2. Send the text message to the device to be located.
3. You receive a text message containing the location of your device.

   Click the link in the text message to display the location of the device in Google Maps.

### 4.4 Lock device and show text message remotely

To lock a lost or stolen device or to send a text message that shall be displayed on the device, you have to send a specific text message from one of the numbers you entered in the **Phone numbers** view in the **Loss & Theft** configuration to the device to be locked.

1. Prepare a text message from one of the numbers you specified in the **Loss & Theft** configuration.
   
   The text message to lock a device is:
   
   \[ \text{lock} \ <\text{Text message password}> \ <\text{optional message}> \]

   **Text message password** is the password you defined in the **Text message password** view of the **Loss & Theft** configuration. **Optional message** is a message that is displayed after the device has been locked.

   For example: `lock MyDevice996 Please Call +43-1111-2222`

2. Send the text message to the device to be locked.

   The device is locked immediately. You receive a text message confirming that the device is locked. If a message has been sent together with the lock command, it is displayed above the lock screen of the device.
4.5 Wipe device remotely

To wipe a device remotely (reset the device to the factory settings via the standard Android wipe functionality), you have to send a specific text message from one of the numbers you entered in the Phone numbers view in the Loss & Theft configuration.

1. Prepare a text message from one of the numbers you specified in the Loss & Theft configuration. The text message to wipe a device is: wipe <Text message password>

   <Text message password> is the password you defined in the Text message password view of the Loss & Theft configuration.

   For example: wipe MyDevice996

2. Send the text message to the device to be wiped.

   You receive a text message confirming that the wipe command will now be executed on the device. The device will then be wiped.

4.6 Get notified on SIM card change

To get notified when the SIM card of your device is changed, activate the SIM change detection feature in the Feature selection view.

This feature detects a SIM card change (for example in a stolen device) and sends a text message to all configured numbers. The text message contains a device description which has to be entered when SIM change detection is activated. The recipient of this message can use the sender telephone number to send for example a locate or lock command to the lost or stolen device.

Note: Remember to disable this feature temporarily before you change your SIM card.

Note: This feature may not work for devices with multiple SIM cards as multiple SIM card support is not a standard Android functionality. Multiple SIM card support is a custom functionality implemented by device manufacturers and therefore varies depending on the manufacturer.
5 Privacy Advisor

Permissions are a central security mechanism of Android that grant an app certain rights. The user can explicitly review these permissions when an app is installed. The Privacy Advisor allows you to filter all apps on a device based upon the permissions they request. These permissions are grouped into three categories:

- **Apps that may cause costs**

  Some apps can cause additional costs which you may not be aware of. Depending upon the permissions an app requests, the app may be able to call premium-rate telephone numbers, change the network state of your phone (which may cause costs when your phone is in roaming) or send text messages without your confirmation.

- **Apps that may harm your privacy**

  Your smartphone or tablet contains private information. Apps with certain permissions can easily read out all of your contacts. You cannot control what the app is actually doing with this information as you have granted the app the permission to do so. Combined with certain connectivity permissions, an app could easily send all your contact information to a third-party without you as the user having to confirm this action. Such apps can harm your privacy!

- **Apps that may access the internet**

  Currently, most of the apps available need permission to connect to the internet. In combination with other permissions, this can be a huge security issue for you. Information that is sent to and received from the internet cannot be monitored. Evaluate if internet access is really needed for an app and if the app is trustworthy!

The Privacy Advisor view lists all apps installed on the device. At the bottom of the view, icons for the three Privacy Advisor filters are displayed. Tap the icons to filter the listed apps.

For example, to only show apps that request permissions related to the category **Apps that may cause costs** select the left-most filter icon. Filters can be combined and will only show apps having permissions related to the filters selected.

If Privacy Advisor filters are selected, the listed apps are ranked based on how the app's permissions are related to the selected filters:

- Apps shown in red: The permissions the app requests indicate a high risk regarding the selected filter.

- Apps shown in yellow: The permissions the app requests indicate a normal risk regarding the selected filter.

- Apps shown in white: The permissions the app requests indicate a low risk regarding the selected filter.

Tap on a list entry to display detailed information about the app. The permissions of the app are listed. In addition, it is described for what these permissions may be used.
If you want to remove the app from your device, tap the **Uninstall** button.
6 Security Advisor

Like any other operating system Android includes several settings that might lead to security risks. The Security Advisor helps you to find these security-related settings. To minimize the vulnerability of your Android device, mind the suggestions shown.

Attention: There are numerous different Android devices on the market which differ in the structure of system settings. The Security Advisor tries to guide you to the right settings.

The Security Advisor lists the security-relevant settings on its start page. It rates the current settings according to the following criteria:

Secure (indicated by a closed green lock icon): The setting ensures the maximum possible security for the device

Insecure (indicated by a open red lock icon): The setting has a value that might lead to security issues. Change the setting if possible.

Unknown (indicated by a question mark icon: The Security Advisor cannot verify if the setting has a secure value. Check the setting manually.

Tap on a setting listed on the start page of the Security Advisor to go to the details page providing a description and the possibility to adjust the setting. Tap Change and adjust the setting in the system settings.

Alternatively, swipe left to navigate through the details pages.
7 Log

In addition to the Android log, Sophos Mobile Security logs important operations in its own log. Especially when the app performs operations in the background, like malware scans when you install other apps, you do not get direct feedback about the results. The Sophos Mobile Security log provides a detailed report about these actions. It reports when these actions were performed and the relevant results.

To display the log, tap the **Action Overflow** or the **Menu** key icon and then tap **Log**.

To clear the log, tap the waste bin icon in the top right-hand corner of the **Log** view.
8 Logging and tracing

Sophos Mobile Security offers extended logging and tracing capabilities. This can be used for troubleshooting when problems with the app occur. It allows to activate more detailed logging and tracing.

To activate the extended logging and tracing capabilities, tap the **Action Overflow** icon in the upper right-hand corner of the **Scanner** view or the **Menu** key and then tap **Settings**.

In the **Trace settings** section of the **Settings** view, you can select **Verbose tracing**. If activated, details of all operations are logged and written to a file together with verbose trace data.

For support reasons you can send this files via email. Tap **Send trace** in the **Settings** view to automatically attach the file to an e-mail in your mail app. An email address from Sophos support is inserted per default.
9 Legal notices

Copyright 2012 Sophos Group. All rights reserved. Sophos is a registered trademark of Sophos Group.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

You find copyright information on third party suppliers in the About dialog of the application.