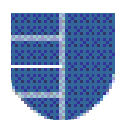


# SOPHOS



**sophos mobile security**

FOR WINDOWS MOBILE

## Configuration Tool user manual

Sophos Mobile Security, version 1.0

Windows Mobile 6

Windows Mobile 5.0

Document date: February 2008





# Contents

- 1 About the Sophos Mobile Security Configuration Tool.....4
- 2 Use the Sophos Mobile Security Configuration Tool.....5
- 3 Close the Sophos Mobile Security Configuration Tool.....6
- 4 Administration tab.....7
- 5 Scans tab.....9
- 6 Updates tab.....11
- 7 Logs tab.....12
- 8 Technical support.....13
- Index .....14

# **1 About the Sophos Mobile Security Configuration Tool**

The Sophos Mobile Security Configuration Tool is a Windows 2000/XP application which allows administrators to create a configuration file containing the Sophos Mobile Security settings to be used on multiple devices.

## **2 Use the Sophos Mobile Security Configuration Tool**

### **1. Configure the Sophos Mobile Security settings**

---

The Sophos Mobile Security Configuration Tool contains a row of tabs. Each tab contains options which are directly related to their counterparts in **Sophos Mobile Security** on the device. Set each of the options as you wish them to operate on the device.

### **2. Save the settings to the configuration file**

---

Click **Save config** to save these settings to a configuration file called **MobileSecurity.cfg** in the **Sophos Mobile Security** application folder.

### **3. Deploy the configuration file**

---

Deploy **MobileSecurity.cfg** to the **My Device** folder on the device. When **Sophos Mobile Security** is installed on the device, it will use the settings in the configuration file.

## 3 Close the Sophos Mobile Security Configuration Tool

- Click **Exit** to close the Sophos Mobile Security Configuration Tool.

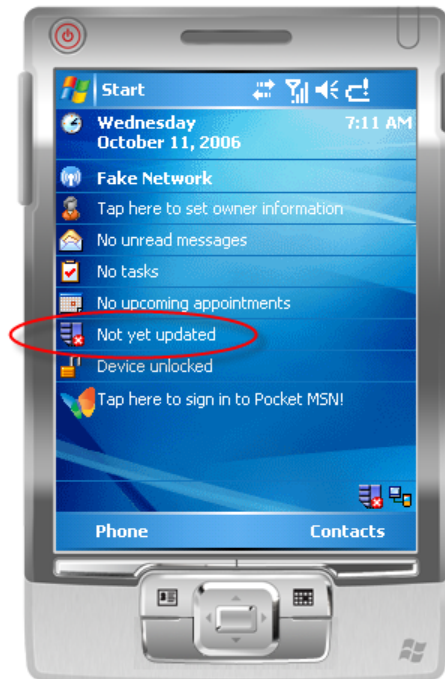


Closing the Sophos Mobile Security Configuration Tool will not save any changes you have made to the configuration file.

## 4 Administration tab

### 4.1 Enable the Today plugin

This option displays Sophos Mobile Security in a section of the device's Today screen.



## 4.2 Add icon to tray

This option displays the Sophos Mobile Security icon in the device's system tray.



## 4.3 Prevent device user configuration

This option prevents the settings in the Sophos Mobile Security Configuration Tool from being displayed by Sophos Mobile Security on the device.

## 5 Scans tab

### 5.1 Create an exclusions list

This option creates an exclusions list, which allows you to exclude certain files and folders from being scanned.

- ¶ To add a file or folder to the exclusions list, type or paste its path in the **Exclusion list** box. For example:

```
\My Documents\My Pictures
```


```
\My Documents\My Pictures\Flower.jpg
```

- ¶ To remove a file or folder from the exclusions list, delete its path from the **Exclusion list** box.

### 5.2 Schedule a scan


You can set up a schedule to run a scan on the device:

1. Select the **Enable scheduled scan** check box.
2. Select the day(s) on which the scan should run.
3. Set the time at which the scan should run.

 Sophos Mobile Security does not need to be open for a scheduled scan to run.


### 5.3 Scan archives during scheduled scanning

- ¶ Under **Scheduled**, select the **Scan archives** check box to scan inside archives during scheduled scanning.

 Scanning archives makes scanning significantly slower.

### 5.4 Scan archives during on-demand scanning

- ¶ Under **On-demand**, select the **Scan archives** check box to scan inside archives during on-demand scanning.

 Scanning archives makes scanning significantly slower.

## 5.5 Ignore the exclusions list during on-demand scanning

The files and folders in the exclusions list are by default not scanned. To **include** the files and folders in the exclusions list during on-demand scanning:

- ☞ Clear the **Apply exclusions list to on-demand scanning** check box.

## 5.6 Configure email reporting

Sophos Mobile Security can send a report by email if a threat is discovered on the device during scanning.

- ☞ To send email reports to the device's Inbox, click **Local Inbox** in the **Email reporting** list.
- ☞ To send email reports to an email address, click **Remote Address** in the **Email reporting** list, then enter the email address in the **Remote email address** box.
- ☞ To send email reports to the device's Inbox and an email address, click **Both** in the **Email reporting** list.
- ☞ To stop sending email reports, click **None** in the **Email reporting** list.

## 5.7 Enable on-access scanning

- ☞ Select the **Enable on-access scanning** check box to scan files as they are opened on the device, and only grant access to those files that do not pose a threat.

## **6 Updates tab**

### **6.1 Enter the update server credentials**

If you are using an update server to download regular updates and keep protection updated on the device, you will need to supply the server credentials.

- ¶ In the **User name** box, type the account name used on the update server.
- ¶ In the **Password** box, type the account password used on the update server.

### **6.2 Schedule automatic updates**

You can set up a schedule to automatically download regular updates to the device from the update server.

1. Select the **Enable scheduled updates** check box.
2. In the **Update every ... hours** box, select an interval between 7 and 24 hours. The default is 7 hours.

### **6.3 Use a billable connection to download updates**

You can allow the device to use a billable connection to download updates if a non-billable connection is not available.

- ¶ Select the **Allow use of billable connection for updates if available** check box.

## **7 Logs tab**

- ¶ In the **Maximum log size (KB)** box, type a maximum size for the log file between 1 and 3072 KB (default 300 KB).
- ¶ In the **Maximum duration (days)** box, type a lifetime for the log file between 7 and 31 days (default 7 days).

## **8 Technical support**

For technical support, visit [www.sophos.com/support](http://www.sophos.com/support).

If you contact technical support, provide as much information as possible, including the following:

- Sophos software version number(s)
- Operating system(s) and patch level(s)
- The device on which the problem was found
- The exact text of any error messages you may have received

# Index

## A

- archives, scanning
  - during on-demand scans 9
  - during scheduled scans 9

## B

- billable connection, using to download updates 11

## C

- closing Sophos Mobile Security Configuration Tool 6
- creating configuration files 5
- credentials, update server
  - entering 11

## D

- deploying configuration files 5
- downloading updates 11

## E

- email reporting, configuring 10
- exclusions list
  - creating 9
  - on-demand scanning, ignoring during 10

## L

- log files
  - maximum age 12
  - maximum size 12

## O

- on-access scanning
  - enabling 10
- on-demand scanning
  - exclusions list, ignoring during 10
  - scheduling 9

## P

- password
  - update server 11
- plugin, Today 7

## S

- saving configuration files 5
- scanning archives
  - during on-demand scans 9
  - during scheduled scans 9
- scheduling scans 9
- Sophos Mobile Security Configuration Tool
  - about 4
  - closing 6
  - using 5

Sophos Mobile Security icon, adding to tray 8

## **T**

Today plugin, enabling 7  
tray, adding Sophos Mobile Security icon 8

## **U**

update server  
    credentials, entering 11  
    password 11  
    user name 11  
updates  
    automatic 11  
    downloading 11  
    scheduling 11  
user configuration, preventing 8  
user name  
    update server 11

Copyright © 2008 Sophos Group. All rights reserved. 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 licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Plc and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.