

UMU SpamSafe for Symbian OS™ User Manual

25 March 2009
Version 1.0

“UMU SpamSafe” is a registered trademark of UMU Limited and UMU SpamSafe product names and symbols/logos are either trademarks or registered trademarks of UMU Limited. All product names referenced herein are trademarks or registered trademarks of their respective companies. UMU Limited disclaims proprietary interest in the marks and names of others. Although UMU Limited makes every effort to ensure that this information is accurate, UMU Limited will not be liable for any errors or omission of facts contained herein. UMU Limited reserves the right to modify specifications cited in this document without prior notice.

Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of UMU Limited.

Copyright ©2008 - 2009 UMU Limited. All rights reserved.

HOW THIS MANUAL IS ORGANISED	4
PDF DOCUMENT	4
FOR MORE INFORMATION.....	4
UMU SPAMSAFE FOR SYMBIAN OS™	5
KEY FEATURES.....	5
INSTALLING UMU SPAMSAFE FOR SYMBIAN OS™	6
ACTIVATING UMU SPAMSAFE FOR SYMBIAN OS™	6
USING UMU SPAMSAFE FOR SYMBIAN OS™	9
<i>Main Screen</i>	9
<i>Settings</i>	9
General Settings.....	10
Whitelist Settings	11
Blacklist Settings.....	11
<i>Exiting</i>	12
<i>Uninstalling</i>	12
TECHNICAL SUPPORT	13
IN PROGRAM.....	13
FREQUENTLY ASKED QUESTIONS	13
EMAIL SUPPORT	13
TELEPHONE SUPPORT	13
ABOUT UMU LIMITED	14
Figure 1 Activation	6
Figure 2 Enter product key	7
Figure 3 License	7
Figure 4 License details.....	8
Figure 5 Privacy screen	8
Figure 6 Main screen.....	9
Figure 7 Settings screen.....	9
Figure 8 General Settings.....	10
Figure 9 Whitelist settings	11
Figure 10 Blacklist settings.....	11

How This Manual is Organised

This User Manual is divided into the following chapters:

Introduction: Provides general information about UMU SpamSafe.

Installing UMU SpamSafe: This section gives instructions on installing UMU SpamSafe onto your device.

Activating UMU SpamSafe: Describes how to activate the product using a provided product key.

Using UMU SpamSafe: Describes how to use UMU SpamSafe.

Technical Support: Describes how to get help with using UMU SpamSafe.

About UMU Limited: Describes the company background and products.

PDF Document

This manual is provided in PDF (Portable Document Format). The PDF document can be used for online viewing and printing using Adobe® Acrobat® Reader. When printing the manual, please print the entire manual, including the copyright and disclaimer statements.

For More Information

Visit UMU Limited at <http://www.umuglobal.com/> for documentation, training, downloads, and service and support contacts.

In our constant attempts to improve our documentation, we would welcome your feedback. If you have any questions, comments, or suggestions about this or any other UMU document, please contact us at documentation@umuglobal.com.

UMU SpamSafe for Symbian OS™

UMU SpamSafe for Symbian OS™ gives you complete control on which messages you want to accept or deny by providing an easy to use application that will help minimise the SPAM you receive. It is compatible with any Symbian OS™ Series 60 2nd Edition or 3rd Edition device.

Key Features

UMU SpamSafe offers the following key features:

- Simple to activate and configure
- Works in one of the following modes:
 - * Off
 - * Whitelist only
 - * Blacklist only
 - * Full
- Trusted by thousands of users worldwide
- Simple over-the-air activation
- Small installed package size
- Low memory footprint
- Low battery drain
- Intuitive user interface

Installing UMU SpamSafe for Symbian OS™

You will be provided with a SIS file. The SIS file can either be installed using the desktop PC Suite software or directly on your device.

Activating UMU SpamSafe for Symbian OS™

Once installed, UMU SpamSafe needs to be activated. In order to activate the program you need to have a SIM card installed and a correctly configured access point that allows internet access from your device.

When UMU SpamSafe first runs, you will be presented with a pop up notification of “Connecting to the internet may be chargeable. Continue?”

If you choose “No”, the application will close but will remain installed on your device. If you wish to continue, choose “Yes” and select the correct access point from the list displayed.

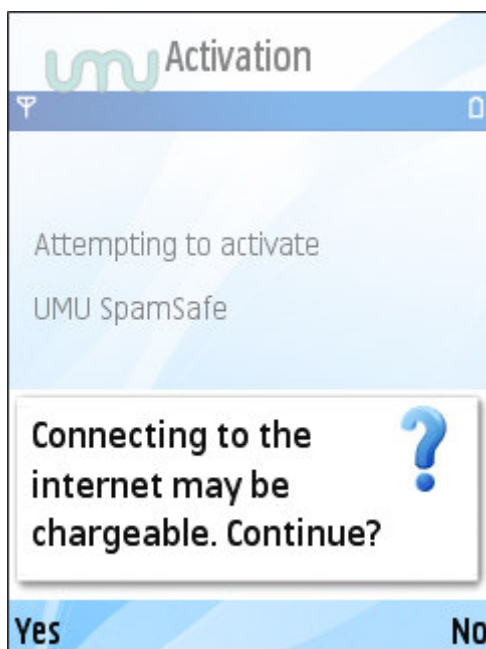


Figure 1 Activation

You will now be prompted to enter your product key; enter the product key you were provided with during your purchase of UMU SpamSafe and then press “Ok”.



Figure 2 Enter product key

Once a valid product key has been entered, the End User License Agreement is displayed and you have two options:

1. If you choose "No", the application will close but will remain installed on your device.
2. If you choose "Yes", a second screen is displayed showing the type of license you have for UMU SpamSafe and when it is due to expire; press "ok" to continue.

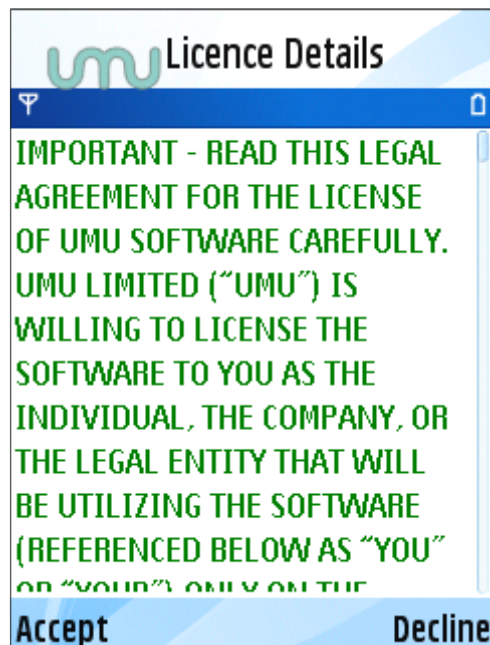


Figure 3 License

Finally, you will be shown your license details.

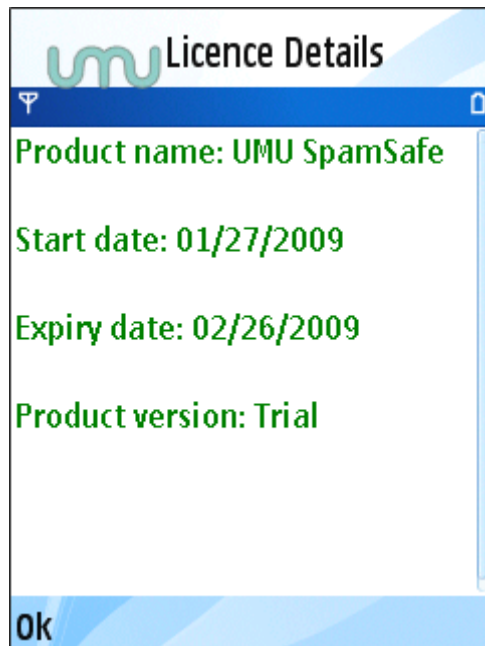


Figure 4 License details

Next, a privacy statement is displayed you have two options:

1. If you choose "No", the application will close but will remain installed on your device.
2. If you choose "Yes", a second screen is displayed where you can choose whether the privacy statement is displayed every time you open UMU SpamSafe.

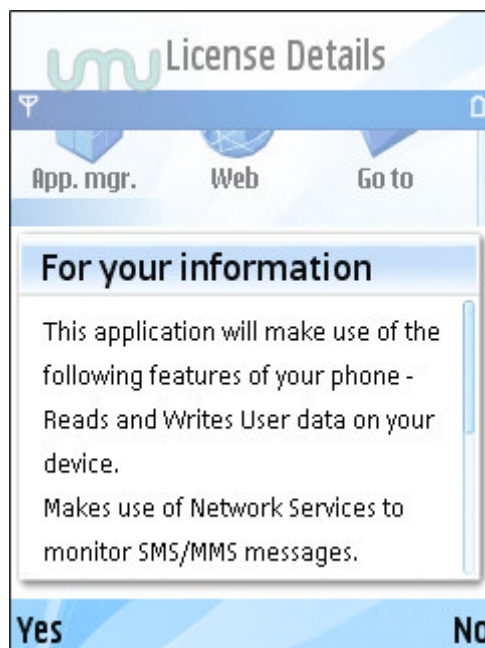


Figure 5 Privacy screen

Using UMU SpamSafe for Symbian OS™

Main Screen

The main screen shows you how many message have been filtered or block by UMU SpamSafe. Initially this will be zero.

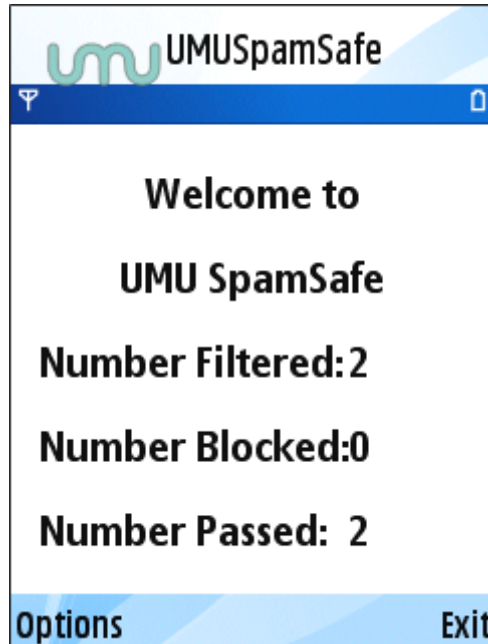


Figure 6 Main screen

Settings

From here, you can get the general settings for initial configuration and then to the blacklist and whitelist to set specific address rules.

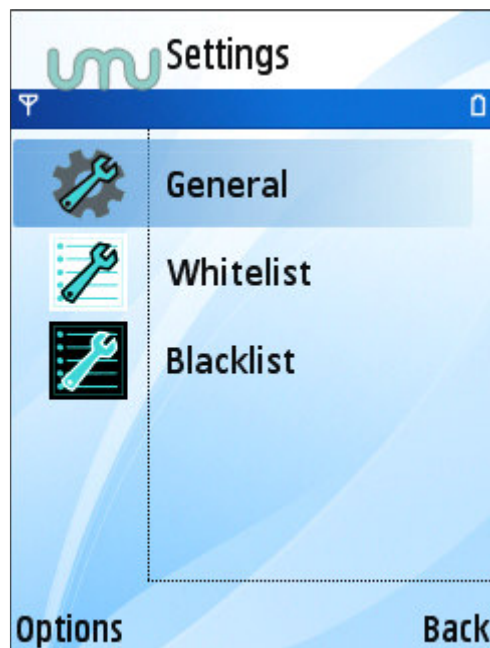


Figure 7 Settings screen

General Settings

From the General Settings area, you can determine in which mode UMU SpamSafe should run, how unidentified senders should be handled and what to do with spam messages when they are filtered.

Mode

There are four modes available:

- Off – In this mode all messages will be accepted as they would normally on this device.
- Whitelist Only – Messages that arrive from addresses not in your contacts list and not in the whitelist are automatically blocked. If the senders address is in your contacts or whitelist the message will be accepted as normal.
- Blacklist Only - Messages that arrive from addresses in the blacklist are automatically blocked. If the senders address is not in your blacklist, the message will be accepted as normal.
- Both – allows numbers on the whitelist, blocks all blacklist numbers and checks unknown numbers with the user

Select the mode that best suits your requirements.

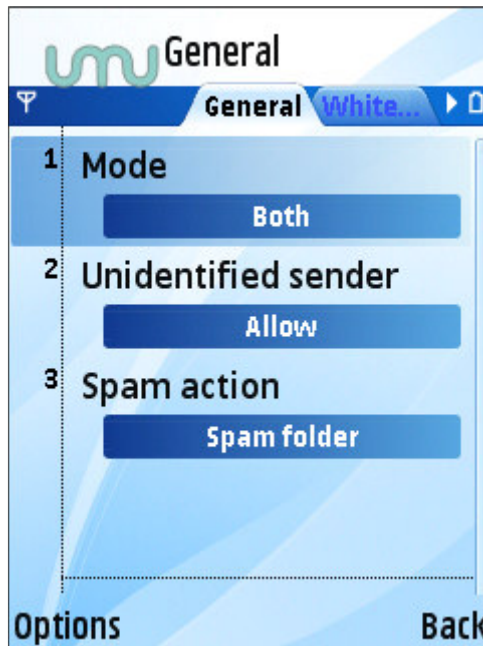


Figure 8 General Settings

Unidentified Sender

This allows you to determine how messages from numbers with no identifiable sender i.e. network messages should be handled. You can choose to either allow them, where they would be accepted as messages normally are on this device or block them, where they are dealt with as per your spam action settings.

Spam Action

This allows you to determine how the messages that are filtered and blocked are handled. Either they can be stored in a spam folder, where you can check them at your leisure or they can be automatically deleted. Note deletion is automatic and permanent; messages filtered and deleted cannot be recovered.



By default mode is set to both, unidentified senders are allowed and spam is sent to the spam folder, this is highly recommended.

Whitelist Settings

The whitelist determines those numbers from whom messages should always be accepted. Your address book is automatically included in the whitelist, although it is not displayed.

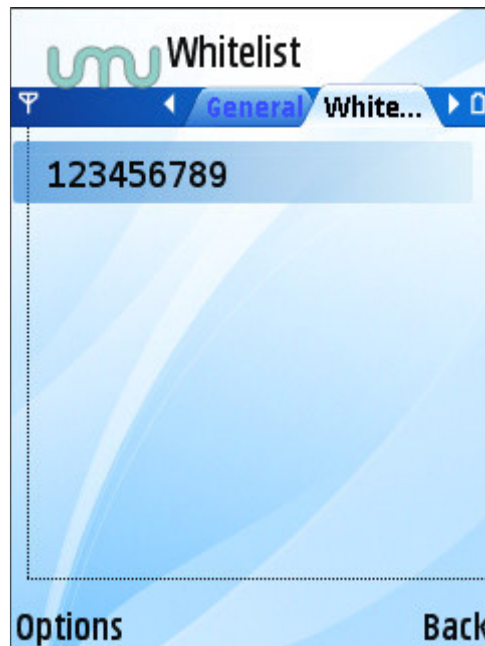


Figure 9 Whitelist settings

Blacklist Settings

The blacklist determines those numbers from whom messages should never be accepted. Where a number is on the blacklist and in your address book, the address book's whitelist status takes priority.

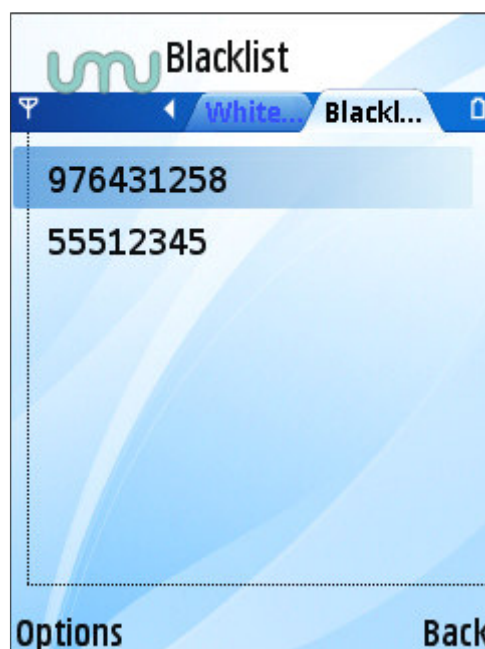


Figure 10 Blacklist settings

Exiting

In order to exit UMU SpamSafe, click on the exit button in the main menu and the program will close but will continue protecting your device in the background.

Uninstalling

In order to uninstall the UMU SpamSafe program, you need to press the Applications key on your device. Then find and run App. Manager and you will be shown a list of programs you have installed. Select UMU SpamSafe, press "Options", and choose "Remove". You will be asked to confirm that you want permanently to remove UMU SpamSafe, if you want to remain protected, press "No"; press "Yes" to remove completely UMU SpamSafe from your device. After you have uninstalled UMU SpamSafe, it will no longer protect your device from unwanted SMS and MMS.

Technical Support

This section gives you instructions on how to find additional technical support.

In program

There is help within the program. From either the main screen or any of the settings menus select "Options" select "Help" and the help page is displayed.

Frequently Asked Questions

You can view a list of frequently asked questions on the internet at <http://www.umuglobal.com/support.php>; this site can also be viewed on your device.

Email Support

If you have a question or problem and cannot find a solution in this manual or the FAQs, you can email the support department at support@umuglobal.com.

We recommend that you check the User Manual and the FAQs on the website before contacting the support department with your question as it may have been answered before.

Telephone Support

If you would like to speak to a member of our support department, please telephone:

+44 (0) 1695 735801

Our telephone support line is open Monday to Friday 9am to 5pm GMT/BST except during public or bank holidays.

If you call outside of these hours, you may leave a message and a member of our support department will get back to you.

About UMU Limited

UMU Limited designs and builds innovative security software for mobile devices running Symbian™ and Windows® Mobile operating systems.

We guarantee to deliver fast responses to security alerts and to tackle any threat to your mobile devices with a system that is easy to use, cost effective and will not drain your battery. We pride ourselves on innovative solutions and customer service, made possible by a dedicated and experienced team of staff.

We are dedicated to mobile security.

Born out of the belief that the AV industry as a whole was failing to offer adequate, focused, and specifically designed protection for mobile devices, UMU Limited was founded in 2004 to address the need for mobile security software. An expanding company based in the North West of England, UMU aims:

- To produce effective, mobile specific security software
- To allow mobile device users to utilise the full capability of their device without fear of infection or intrusion
- To deliver outstanding ease of use
- To deliver swift responses to security alerts

Dependable mobile security solutions are only as good as the research and development that have been expended upon them. With this in mind, UMU is a mobile only software provider so we are not constrained or distracted by desktop PC or server software requirements and footprints.

Friendly, Professional and Approachable

We are an ethical company who have produced the solutions that we feel are important and we have a friendly, professional and approachable team. We have not 'cut down' existing desktop PC or server software for use on mobile devices. All of UMU's software is developed in-house specifically for mobile devices, guaranteeing dedication to the customer's needs and requirements and the most efficient and effective software available.

Visit our website at <http://www.umuglobal.com/> to learn more about products, our services, and us.