Norton™ Smartphone Security User's Guide

for Symbian OS™

symantec™

Legal Notice

Symantec, the Symantec Logo, LiveUpdate, Symantec AntiVirus, Symantec Client Firewall, Symantec SMS AntiSpam and Norton Smartphone Security are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Symbian and Symbian OS are registered trademarks of Symbian Software Ltd. Windows is a registered trademark of Microsoft Corporation.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

http://www.symantec.com

Contents

Service and support solutions

Chapter 1 Introducing Norton Smartphone Security

Chapter 2 Installing Norton Smartphone Security

Chapter 3 Protecting devices with Norton Smartphone Security

Chapter 4 Updating devices

Index

Service and support solutions

About online support

Symantec offers a range of technical support and customer service options. You can access these options by clicking the Support link anywhere in the product, or by pointing your Web browser to the following address:

www.symantec.com/techsupp/

Under the Home & Home Office section, select your product. Then, from the list of options, choose the item that best describes your issue.

The Symantec Web site also contains answers to the most common customer questions.

Note: If you received this product when you purchased your computer, your computer manufacturer may be responsible for providing your support.

About phone support

If you have a question or problem that you cannot resolve on the support Web site by yourself, the Web site provides a link to information about phone support. For questions about installation or common problems on a current version of a Norton product, there is no charge. For other problems, or if you are using an older version, phone support will be fee-based. This support is available to all registered customers.

To visit our Customer Support site, go to:

www.symantec.com/techsupp/

Under the Home & Home Office section, select your product. Then, from the list of options, choose the item that best describes your issue. If you have a question or problem that you still cannot resolve on the support Web site by yourself, click a Contact Us link for additional phone support information. This support is available to all registered customers.

Support for old and discontinued versions

When Symantec announces that a product will no longer be marketed or sold, telephone support is discontinued six months after the termination announcement. Technical information on these products may still be available through the support Web site at the following address:

www.symantec.com/techsupp/

Subscription policy

This renewable service includes protection updates and new product features as available throughout the service period. Please note that features may be added, modified, or removed during the service period.

Service period lengths vary by Symantec product. After your initial service period ends, you must renew your service subscription before you can update and use your protection. When you run LiveUpdate near the end of your service period, you are prompted to subscribe for a nominal charge. Follow the instructions on the screen to renew.

Worldwide service and support

Support solutions vary by country. For Symantec and International Partner locations that are outside of the United States, contact one of the service and support offices that are listed in this section. You can also go to the following Web site and select your language:

www.symantec.com/techsupp/globalsupport.html

For each region, please check the Web site for the appropriate phone number.

Region	Contact information
North America	■ Symantec Corporation 555 International Way Springfield, OR 97477 U.S.A. http://www.symantec.com/home_homeoffice/support/index.jsp
Australia and New Zealand	■ Symantec Australia Level 2, 1 Julius Avenue North Ryde, NSW 2113 Sydney Australia http://www.symantec.com/en/aa/home_homeoffice/support/index.jsp
Europe, Middle East, and Africa	■ Symantec Ltd Consumer Services & Support PO Box 5689 Blanchardstown Dublin 15 Ireland http://www.symantec.com/en/uk/home_homeoffice/support/index.jsp
Latin America	■ Symantec Brasil Sevico e Suporte Symantec Caixa Postal 3037 CEP 06210-970 Brasil ■ Portuguese language support: http://www.symantec.com/pt/br/home_homeoffice/support/index.jsp ■ Spanish language support: http://www.symantec.com/es/mx/home_homeoffice/support/index.jsp

August 01, 2007

Chapter 1

Introducing Norton Smartphone Security

This chapter includes the following topics:

- About Norton Smartphone Security
- How Norton Smartphone Security works
- Where to get more information

About Norton Smartphone Security

Norton Smartphone Security provides secure mobile computing through comprehensive, reliable protection against malicious attacks that are directed at mobile devices.

Norton Smartphone Security includes the following components and features:

- AntiVirus protection: Award-winning Symantec AntiVirus technologies automatically scan, detect, and quarantine harmful viruses and worms.
- AntiSpam for SMS: SMS spam messages are automatically placed in Spam folder or deleted, and you can configure which messages should be treated as spam.
- Firewall protection: Prevent intruders from entering and exporting data from your device.
- LiveUpdate support: Product and virus definition updates delivered wirelessly via LiveUpdate or via cradle synchronization.
- Protects against malicious code downloaded from the Web, sent via email or a Wi-Fi connection, or beamed via Bluetooth® or infrared ports.
- Supports the ability to schedule antivirus scans on your device.

- On-demand scans allow you to check for viruses in individual files, file archives, and applications.
- Activity log shows all recently logged events to ensure users are aware of potential risks.

How Norton Smartphone Security works

The Norton Smartphone Security components work together to protect the devices from threats.

To understand how Norton Smartphone Security works, you need to know the following:

- How the devices are protected
- How threat protection and Norton Smartphone Security are updated
- How activities are logged

How the devices are protected

Norton Smartphone Security uses virus definitions files to identify known threats. As files are accessed on the device, Auto-Protect provides automatic, real-time threat scanning. Users can also perform on-demand scans. By default, when Auto-Protect detects a suspicious file, it sends the file to the Quarantine. Infected files in the Quarantine are secure and cannot spread threats into other areas of the device.

If the first default action fails (Quarantine), a second default action (Deny Access) denies any application from opening the files.

See Table 3-2 on page 19.

What happens when the firewall detects unauthorized activity

When the Norton Smartphone Security firewall detects an unauthorized activity such as inbound or outbound connections or port scanning attempts, it does the following:

- On some devices, if configured, may temporarily display a message on the screen that provides information about the unauthorized activity
- Logs the firewall activity in the Activity Log
  See “About the Activity Log” on page 22.
- Port scan detection blocks all traffic from that IP address.

How threat protection and Norton Smartphone Security are updated

Symantec™ Security Response provides users with regular updates to virus definitions files to keep their virus protection current. In addition, Symantec may also provide software updates to Norton Smartphone Security.

You obtain virus definitions and product updates directly from the Symantec LiveUpdate server.

See "Updating devices" on page 27.

How activities are logged

The Norton Smartphone Security software on the device records information about the antivirus and firewall activities that are performed on the device. It also records information about the updates.

Users can view this data directly on the device.

See "About the Activity Log" on page 22.

Where to get more information

On-device Help is installed with the product software on the devices.

On the Symantec Support Web site, you can find the latest protection and program updates, patches, online tutorials, Knowledge Base articles, and threat removal tools.

To explore the Symantec Support Web site

1. On the Internet, go to the following URL:

   http://www.symantec.com

2. Follow the links to the information that you want.

Chapter 2

Installing Norton Smartphone Security

This chapter includes the following topics:

- System requirements
- Installing Norton Smartphone Security
- Testing the installation
- Upgrading Norton Smartphone Security
- Uninstalling Norton Smartphone Security

System requirements

Table 2-1 describes the system requirements for the devices. Desktop platforms that support Norton Smartphone Security are Windows XP Home/Professional with Service Pack 2, and Windows Vista.

Table 2-1 Device requirements

Operating system or component	Requirements
Symbian OS 9	Includes Nokia Series 60 Version 3 devices such as: ■ Nokia E50 ■ Nokia E60 ■ Nokia E61 ■ Nokia E62 ■ Nokia E70 ■ Nokia N71 ■ Nokia N73 ■ Nokia N80 ■ Nokia N91 ■ Nokia N93 ■ Nokia 3250 ■ Nokia 5500 Includes UIQ 3.0 devices such as: ■ Sony Ericsson P990 ■ Sony Ericsson M600i ■ Sony Ericsson W950
Devices	Installation footprint: 1.1 MB
Symantec LiveUpdate Wireless	Wireless Internet hardware support using the built-in TCP/IP stack.

Installing Norton Smartphone Security

Once you connect your device to your desktop computer, you can install by using the installation wizard on the CD, and then synchronize the device with your desktop computer.

Before installation, do the following on the device:

- Set the device clock to the current date and time
- Close all files
- Exit all applications
- Restart the device to ensure that previously installed applications are fully installed and that data is saved.

Note: Installation to the default directory is the only supported installation configuration.

To install Norton Smartphone Security

1. Insert the CD and run the start.exe file.
2. Select **Install Norton Smartphone Security**.
3. Follow the on-screen instructions to complete the installation.

   Do not cancel or interrupt the installation process. After the installation successful message, you are prompted to restart the device. An icon for Norton appears on the device after installation is complete.

Testing the installation

You can verify that Norton Smartphone Security is active by downloading the standard European Institute for Computer Anti-Virus Research (EICAR) test file, and copying it to the device.

To test the installation

1. Download the EICAR test file from the following URL:

   www.eicar.org

   You may need to temporarily disable threat scanning on your computer to access the EICAR test file. Make sure that you re-enable threat scanning on your computer after you are finished.
2. Copy the EICAR file to the device.

   A successful installation of Norton Smartphone Security displays a dialog box when the EICAR test file is copied to the device.

Upgrading Norton Smartphone Security

Do the following before upgrading:

- Set the device clock to the current date and time
- Close all files
- Exit all applications
- Backup your data
- Restart the device to ensure that previously installed applications are fully installed and data is saved

Installing the upgrade

Use the following procedure to install the upgrade.

To install the upgrade

1. Insert the CD and run the start.exe file.
2. Select **Install Norton Smartphone Security**.
3. Follow the on-screen instructions to complete the installation.
4. If you receive a message saying that the upgrade is unable to remove the previous version of the software, click **OK** to continue.

   Do not cancel or interrupt the installation process.

Uninstalling Norton Smartphone Security

While it is possible to uninstall individual components of Norton Smartphone Security, doing so causes Norton Smartphone Security to fail. If you need to reinstall Norton Smartphone Security, you must first uninstall all components.

To uninstall Norton Smartphone Security on the devices

1. Open the device's application manager.
2. In the Application manager dialog box, select **Norton Security**, and then select **Remove**.
3. Restart the device.

Chapter 3

Protecting devices with Norton Smartphone Security

This chapter includes the following topics:

- Open Norton Smartphone Security
- About scanning for and responding to threats
- About Auto-Protect scans
- Configure firewall protection
- About the Activity Log
- About SMS AntiSpam

Open Norton Smartphone Security

Norton Smartphone Security protects the device on which it is installed. You do not have to start the program to be protected.

To open Norton Smartphone Security

◆ On your device, open the **Norton** icon.

About the options available from the main view

Table 3-1 describes the Norton Smartphone Security main view, which lets you access program components and change settings. The items listed in the table are accessed through the AntiVirus menu option. The menu contents are similar, whatever application (AntiVirus, Firewall, LiveUpdate, SMS AntiSpam) you hightlight.

Table 3-1 Main view options

Option	Description
AntiVirus	
- Scan	Manually scan the device for viruses
- Activity log	View information about scan
- Quarantine list	View the list of quarantine
- Threats list	View the list of threats from which your device is currently protected
- Settings	Turn Auto-Protect and firewall off or on, and customize firewall and LiveUpdate setting
Scan	Manually scan the device for viruses
Search for updates	Search for product and virus definitions updates
Activity log	
- AntiVirus	View information about antivirus scans
- Firewall	View information about the firewall
- LiveUpdate	View information about LiveUpdate schedule
Settings	
- AntiVirus	View and set parameters for AntiVirus scan; turn on/off Auto-Protect
- Firewall	Customize firewall settings
- LiveUpdate	Schedule LiveUpdates
- SMS AntiSpam	Set rules for SMS AntiSpam
Subscription	Update your product subscription
About	Display product, version, and licensing information
License agreement	Display information about the license agreement
Help	Display online Help for Norton Smartphone Security

Table 3-1 Main view options *(continued)*

Option	Description
Exit	Exit from Norton Smartphone Security

About scanning for and responding to threats

When Norton Smartphone Security detects a threat, the user can take an action. The type of action that the user takes depends on the nature of the threat.

Scheduling scans

Scheduled scans automatically check for viruses on your device. Reminders that you set, as well as the default setting, prompt you to run a scan.

You can enable and configure scheduled scans to occur at a specified interval.

To schedule a scan

1. On your device, open the **Norton** icon.
2. Depending on your device, do one of the following:
   - Select **Options** > **Settings** > **AntiVirus** > **Scheduled scan**.
   - Select **AntiVirus** > **Settings** > **Scheduled scan**.
3. In the dialog box, cycle through the options until the preferred options appear, and then set the time and date if necessary.

About Auto-Protect scans

As users access files on the devices, Auto-Protect provides real-time threat scanning. By default, when Auto-Protect detects a suspicious file, it moves the file to the Quarantine. Infected files in the Quarantine are secure and cannot spread threats into other areas of the device.

If the automatic action fails, the next action is Deny Access.

Table 3-2 describes the automatic actions that are available.

Table 3-2 Automatic actions

Action	Description
Deny Access	Does not allow any application to open the infected file.

Table 3-2 Automatic actions *(continued)*

Action	Description
Delete	Deletes the infected file and is the recommended action
Quarantine	(Default) Moves the infected file to the Quarantine
Repair	Lets you know whether a threat is repairable or not.
Prompt	Displays a prompt for an action.

Temporarily turn off Auto-Protect

Auto-Protect monitors and scans the files that the device accesses. When a threat or suspicious activity is detected, the potentially malicious file is blocked, and it performs the action you selected in Table 3-2 on page 19.

By default, Auto-Protect is turned on. It is recommended that Auto-Protect remain turned on at all times.

To turn off Auto-Protect

1. On your device, select the **Norton** icon.
2. Depending on your device, do one of the following:
   - Select **Options > Settings > AntiVirus > Auto-Protect**.
   - Select **AntiVirus > Settings > Auto-Protect**.
3. Select **Off**.

Configure firewall protection

Norton Smartphone Security provides preconfigured options for your immediate protection. You can also customize firewall protection by selecting the way you want to handle inbound and outbound traffic on your device.

Selecting one of the following preconfigured options is adequate for most users:

- Low (default): All outbound services are permitted; all inbound services are permitted.
- Medium: All outbound services are permitted; all inbound services are blocked.
- High: All common outbound services are permitted; all inbound services are blocked.

To select a preconfigured firewall option

1. On your device, open the **Norton** icon.
2. Depending on your device, do one of the following:
   - Select **Options > Settings > Firewall**.
   - Select **Firewall > Settings**.
3. In the dialog box, select the preferred firewall level.

Temporarily turn off firewall protection

Firewall protection protects the device from Internet attacks, dangerous Web content, port scans, and other suspicious behavior.

By default, firewall protection is turned on, and it is recommended that it remain turned on at all times.

There may be times when you want to temporarily disable firewall protection. For example, you might want to see if the firewall is preventing a Web page from appearing correctly.

Note: Turning off firewall protection disables all of the customized settings and the device is no longer safe from Internet attacks.

To turn off firewall protection

1. On your device, open the **Norton** icon.
2. Do one of the following:
   - Select **Options > Settings > Firewall**.
   - Select **Firewall > Settings**.
3. Select **Protection Level > None**.

To turn on firewall protection

1. On your device, open the **Norton Security** icon.
2. Do one of the following:
   - Select **Options > Settings > Firewall**.
   - Select **Firewall > Settings**.
3. Select **Protection Level > Low, Medium, or High**.

About the Activity Log

The device maintains a local history of antivirus, firewall, and LiveUpdate activity.

Threat-related activities

The following threat-related activities are recorded by the device:

Partial scan	An entry is added when users cancel a scan or scan only part of the device.
Full scan	A full scan entry is added when the device, including storage cards, is scanned.
Found threat	A found threat entry is added whenever Norton Smartphone Security identifies a file that is infected with a threat. Included in this entry is the action that was taken on the infected file.

Norton Smartphone Security logs the following Quarantine events:

- Quarantine add
- Quarantine delete
- Quarantine restore

For each Quarantine event, the following details are provided:

- Date
- Time
- Event (for example, add, delete, or restore)
- Source (for example, scanner, Auto-Protect, or Quarantine)
- File
- Status (for example, successful or unsuccessful)

Firewall-related activities

The following firewall-related activities are recorded by the device:

Blocked outbound TCP connection	An entry is added when a blocked outbound TCP connection is attempted.
Blocked inbound TCP connection	An entry is added when a blocked inbound TCP connection is attempted.

Port scanning attempt	An entry is added when port scanning is attempted.

For each firewall-related activity, the log provides the following details:

- Date of occurrence
- Time of occurrence
- Protocol involved (TCP only)
- Direction (Outbound/Inbound)
- Source IP address
- Source port
- Destination IP address
- Destination port

Note: The amount of firewall log entries within a specified time interval is limited. If there are a large number of events in a short time, only a subset of these events are logged.

LiveUpdate-related activities

The following LiveUpdate-related activities are recorded by the device:

Application Update	Provides information on updates to antivirus, firewall, and LiveUpdate components. Also includes information on SMS AntiSpam, such as date and time, component name, before and after version numbers, and status of operation.
Virus Definition Update	Provides information on old virus definitions version and new virus definitions version. Details include date and time, before and after sequence number, and status of operation.

When the log is full

When the Activity Log reaches 300 KB in size, Norton Smartphone Security first compacts the log file, which creates more space. If compacting the log file does not create enough space, entries are deleted (oldest first) until the size drops below 300 KB.

About SMS AntiSpam

SMS AntiSpam works by allowing you to classify an incoming SMS message as spam or not, and if it is spam, to move the message to a folder reserved for spam messages. You can create one or more rules for recognizing an incoming SMS message as matching certain conditions, and for taking a specified action if it does.

The main display for AntiSpam settings is a list of rules that you create. The list displays the name you create for each rule, and a small icon indicating the action of the rule.

The last rule matching an incoming message is the rule that applies to that message. If there is no rule established, the message is routed to the Inbox.

Table 3-3 lists the options you use to create and modify rules.

Table 3-3 Rule options

Rule options	Description
Open	Edit the selected rule
New rule	Add a new rule
Move up	Move the selected rule up one position on the list
Move down	Move the selected rule down one position on the list
Delete	Delete the selected rule
Help	Show the help application for the display
Exit	Exit the application

Once you establish a rule for a contact, you can specify certain details for that rule. You can give the rule a name, set a condition, and specify an action if the condition is met.

Table 3-4 lists the rule detail options that you can apply to rules you create.

Table 3-4 Rule detail options

Detail options	Description
Name	Create a name for the rule.

Table 3-4 Rule detail options *(continued)*

Detail options	Description
Condition	In contacts: Message from any person or company in the contacts database. Not in contacts: Message from any person or company that is not in the contacts database. From contact: Message from a specified person or company that you select from the contacts database. From group (or category or folder) : Message from a specified person or company that you identify as a group in the contacts database. From any: Message from any phone number. From number: Message from a phone number that you specify. From annonymous: Message has no phone number in it. Contains text: Message contains text that you specify. The text is case-insensitive. Not matched: Message not matched to any rule.
Action	Accept the message with no further action; it remains in the inbox. Move to: Accept the message and move it to a folder that you specify. Delete: Delete the message.

Setting up SMS AntiSpam rules and conditions

You can establish rules for incoming SMS messages, and set up conditions for each rule. You can also edit or modify existing rules and conditions through the rule dialog box.

To set up SMS AntiSpam rules and conditions

1. On your device, select the **Norton** icon.
2. Depending on your device, do one of the following:
   - Select **Options** > **Settings** > **SMS AntiSpam** > **Options** > **New rule**.
   - Select **SMS AntiSpam** > **More** > **New rule**.
3. Enter the name, condition and action for the rule in the rule details dialog box.
4. Repeat steps 2 and 3 as necessary to create additional rules and conditions.

Phone number matching

The spam filter compares the incoming message phone number with existing contact phone numbers, starting from right to left. Thecompare process may match more than one phone number. If at least one match is found, then the AntiSpam rule is applied.

Chapter 4

Updating devices

This chapter includes the following topics:

- Updating devices
- Scheduling updates or reminders
- Updating the product subscription

Updating devices

You can regularly download and install the latest virus definitions on your device to protect your device from current threats.

Norton Smartphone Security supports virus definitions file updates. Symantec products use virus definitions files to identify threats. Symantec Security Response researches and responds to new threats and provides customers with updates of virus definitions files as new threats emerge.

If the device does not have an active Internet connection, LiveUpdate tries to create a network connection. The connection fails if the device isn't configured with an Internet access point.

Norton Smartphone Security supports the following types of updates:

Virus definitions file updates	Symantec products use virus definitions files to identify threats. Symantec Security Response researches and responds to new threats and provides customers with updates of virus definitions files as new threats emerge.
Engine updates	Symantec occasionally provides antivirus scan engine updates to take into account new types of threats that have been identified.

To search for updates

1. On your device, select the **Norton** icon.
2. Depending on your device, do one of the following:
    - Select **Options > Search for updates**.
    - Select **LiveUpdate > Search for updates**.

LiveUpdate connects to the Symantec LiveUpdate server, where it searches for available virus definitions files, software, and engine updates.

After you update your device with the latest virus definitions file, your device is protected from the most current threats.

Scheduling updates or reminders

Scheduled updates automatically check for and install updates for every component on the device, including virus definitions files. Reminders that you set, as well as default reminders, prompt you to check for updates.

To schedule updates

1. On your device, open the **Norton** icon.
2. Depending on your device, do one of the following:
    - Select **Options > Settings > LiveUpdate**.
    - Select **LiveUpdate > Settings**.
3. In the dialog box, cycle through the options until the preferred options appear, and then set the time and date if necessary.

Updating the product subscription

You can easily update the Norton Smartphone Security subscription through the main menu. If the subscription has expired, you receive a message on your phone to renew the license.

Note: Make sure you have configured internet service on your phone before proceeding. Refer to your wireless service provider for more information.

To update the product subscription

1. On your device, select the **Norton** icon.
2. Depending on your device, do one of the following:

- Select **Options > Subscription**.
- Select **Subscription** from the main menu.

3 Select **Yes** to update the subscription.

4 Select your internet connection from the list. This may take several moments to connect to the internet server.

5 Select the payment option.

6 Follow the instructions on the subscription wizard to complete the renewal process.

Index