



**FortiClient Host Security for Symbian OS
Version 3.0**

FORTINET™

www.fortinet.com

FortiClient Host Security for Symbian OS User Guide
Version 3.0
March 19, 2007
04-30000-0251-20070319

© Copyright 2007 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiAnalyzer, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction	5
About FortiClient Host Security for Symbian OS	5
Documentation.....	5
Fortinet Knowledge Center	5
Comments on Fortinet technical documentation.....	5
Customer service and technical support.....	6
Installation	7
Supported software/hardware platforms.....	7
Installing the FortiClient program	7
To install from the FortiClient SIS file	7
Starting the FortiClient program	7
To start the FortiClient program.....	7
Configuration.....	9
FortiClient window.....	9
FortiTray	9
To enable or disable FortiTray.....	9
Antivirus	10
To launch a manual AV scan of all files on the mobile device.....	10
To scan files in a specified directory.....	10
To set an AV scan schedule	10
To enable real-time protection	10
To change Antivirus settings.....	10
Update.....	11
To initiate an immediate update.....	11
To select the connection for updates.....	11
To enable or disable the license renewal warning.....	11
To set an update schedule	11
Antispam	12
To enable SMS Filter features	12
To view the Spam log	12
Configuring blacklist and whitelist	12
To configure the blacklist.....	12
To configure the whitelist.....	13
Incoming call filter	13
To view incoming call filter status	13
To reset rejected calls total.....	13
To set the Filter Mode.....	13
To set the Default Action	14
To manage SMS templates	15

Configuring blacklist and whitelist	16
To configure the blacklist	16
To configure the whitelist	16
Working with greetings	17
To record a greeting	17
To import a greeting	17
To manage greetings	17
Firewall	18
To enable firewall and set the protection level	18
Logs	18
To manage logs	18
Quarantine	19
To view and manage the virus affected files	19
To configure quarantine settings	19
Viewing version number	19
Index	21

Introduction

This chapter introduces you to FortiClient Host Security for Symbian OS and the following topics:

- [About FortiClient Host Security for Symbian OS](#)
- [Documentation](#)
- [Customer service and technical support](#)

About FortiClient Host Security for Symbian OS

The FortiClient Host Security for Symbian OS is a PDA-based program to protect your mobile devices running Symbian OS from virus and spam attacks.

The FortiClient program has the following features:

- Antivirus -- supports both on-demand and real-time AV scanning. It also supports manual and automatic updates of AV engine and signatures. The virus affected files are sent to the quarantine folder.
- SMS antispam -- blocks unwanted SMS messages.
- Firewall protection -- protects your Internet, such as HTTP and HTTPS, and email traffic.
- Logging -- records all AV detection and other events.

Documentation

In addition to this *FortiClient Host Security for Symbian User Guide*, the FortiClient online help provides information and procedures for using and configuring the FortiClient program.

Fortinet Knowledge Center

The most recent Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains short how-to articles, FAQs, technical notes, product and feature guides, and much more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

Comments on Fortinet technical documentation

You can send information about errors or omissions in this document or any Fortinet technical documentation to techdoc@fortinet.com.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at <http://support.fortinet.com> to learn about the technical support services that Fortinet provides.

Installation

This section describes how to install the FortiClient program onto your mobile devices.

The following topics are included in this section:

- [Supported software/hardware platforms](#)
- [Installing the FortiClient program](#)
- [Starting the FortiClient program](#)

Supported software/hardware platforms

Symbian S60 OS 7.0/8.0:

- Nokia models 3230, 6260, 6600, 6630, 7610, N70

Symbian S60 OS 9.0:

- Nokia 3250

Symbian UIQ OS 2.0/2.1:

- Sony Ericsson P910c, Nokia 6708

Symbian UIQ OS 3.0:

- Sony Ericsson M608

Installing the FortiClient program

Install the FortiClient program onto your mobile device from the FortiClient SIS file.

To install from the FortiClient SIS file

- 1 Download the FortiClient SIS file to your PC.
- 2 On your PC, install your mobile device's PC suite software.
- 3 Connect your mobile device to your PC.
- 4 Start the device's PC suite software.
- 5 Select Install Applications to install the FortiClient program.
- 6 Follow the instructions on your PC and phone screens.

Starting the FortiClient program

The following procedure applies to Nokia 6620 cellular phone. For other cellular phone models, the procedure may vary, but should be similar.

To start the FortiClient program

- 1 On your mobile device, press Menu.
- 2 Select FortiClient.

Configuration

This section describes how to use the following FortiClient features:

- [FortiClient window](#)
- [FortiTray](#)
- [Antivirus](#)
- [Update](#)
- [Antispam](#)
- [Incoming call filter](#)
- [Firewall](#)
- [Logs](#)
- [Quarantine](#)
- [Viewing version number](#)





FortiClient window

You can access the FortiClient window at any time, even while using another application. Press the Edit key and * at the same time. When you have finished working with the FortiClient application, select Exit to return to your previous application.

FortiTray

If FortiTray is enabled, four icons at the top right of your device screen display the status of the FortiClient application at all times.

Table 1: FortiClient FortiTray icons

	Real-time Protection is enabled.
	Incoming Call Filter is enabled
	Active SMS Filter is enabled.
	Active Firewall is enabled.

To enable or disable FortiTray

- 1 Start the FortiClient application.
- 2 Select **Options > Settings > Anti Virus**.
- 3 With the joystick, set Display Trayicon On or Off.

Antivirus

The FortiClient program protects your mobile device from virus attacks. It supports both manual and scheduled file scanning. Use manual scanning to scan files for virus infections anytime you want. You can also schedule times to scan files. (See [“To set an AV scan schedule” on page 10](#)).

If Quarantine is enabled (see [“Quarantine” on page 19](#)), infected files are moved to the Quarantine area. Otherwise, infected files are deleted.

To launch a manual AV scan of all files on the mobile device

- 1 Do one of the following:
 - Select **Scan**.
 - Select **Options > Scan > Full Scan**.

The scanning process starts. Once it is done, the scanning result appears.

- 2 Select OK.

To scan files in a specified directory

Custom scan is not available on UIQ 3.0 devices.

- 1 Select **Options > Scan > Custom Scan**.
- 2 Navigate to the directory that you want to scan, using the joystick.
- 3 Select OK.

To set an AV scan schedule

- 1 Select **Options > Settings**, then **Options > Antivirus > Schedule Scan**.
- 2 Set the Scan Frequency and options to one of the following:
 - Never
 - Daily + Start Time
 - Weekly + Start Time + Day
 - Monthly + Start Time + Date

To enable real-time protection

- 1 Select **Options > Settings > Anti Virus**.
- 2 Using the joystick, set Real-time Protection to On.

To change Antivirus settings

- 1 Select **Options > Settings > Anti Virus** or select **Options > Settings** and then **Options > Anti Virus > General Settings**.
- 2 Using the joystick, set the following options:

Real-time Protection	Set to On to scan files as they are accessed.
On Found Virus	Select action to take when a virus is found: ask user - ask user to choose deny access or delete deny access - block access to file delete - delete the file
Display Trayicon	Set to On to show icon when a virus is found.
Enable Sound	Set to On to play a sound when a virus is found.

Update

To keep the AV signatures and AV engine up-to-date, whenever a wireless connection is established, your device will check the database server and get updates from the server.

You can initiate an update any time you like. You can also schedule an update (See ["To set an update schedule" on page 11](#)).

You can view the current AV signature and AV engine version information on the Update page.

To initiate an immediate update

- 1 Select **Options > Update**.
 - 2 Select **Options > Start**.
 - 3 If asked, select the access point.
- The update status bar displays the update progress.

To select the connection for updates

- 1 Select **Options > Settings > Update**.
- 2 Use the joystick to select the default connection. If you do not always use the same connection for updates, select Always Ask.



Note: After a successful update, the access point you used is saved as the default.

To enable or disable the license renewal warning

- 1 Select **Options > Settings > Update**.
- 2 Set Bill Prompt to Yes or No using the joystick.

To set an update schedule

- 1 Select **Options > Settings** and then select **Options > Update > Schedule Update**.
- 2 Set the Update Frequency and options to one of the following:
 - Never
 - Daily + Start Time
 - Weekly + Start Time + Day
 - Monthly + Start Time + Date

Antispam

Using the FortiClient program, you can block unwanted Short Message Service (SMS) messages. You can also block unwanted phone numbers by blacklisting them and accept numbers that are not in your contact list by whitelisting them.

To enable SMS Filter features

- 1 Select **Options > Settings > Anti Spam**.
- 2 Using the joystick, set the following options:

Active SMS Filter	Set On to block unwanted SMS messages, otherwise set Off.
Action	
Smart filter	Reject message if sender is not in the contact list or whitelist, or is in the blacklist.
Reject blacklist only	Reject message only if sender is in blacklist.
Accept whitelist only	Reject message unless sender is in whitelist.
Reject all	Block all SMS messages.
Discard method	(Global edition only)
Delete	Delete rejected messages.
Move to trash	Move rejected messages to the Trash folder.

To view the Spam log

- 1 Do one of the following:
 - Select **Spam**.
 - Select **Options > View Log > Spam log**.

Configuring blacklist and whitelist

You can list undesired SMS message senders in the blacklist and permitted senders in the whitelist.



Note: In both blacklist and whitelist entries, you can use wildcard characters in phone numbers. "?" replaces any single digit. "*" replaces multiple digits.

To configure the blacklist

- 1 Select **Options > Settings**.
- 2 Select **Options > Antispam > Blacklist**.
- 3 Do one of the following:
 - To block a number, select **Options > Add Item**. Type the unwanted user name and phone number, and select OK.
 - To block a number that is in your contact list, select **Options > From Phonebook**. Using the joystick, highlight the contact to block. Select **Options > Mark/Unmark > Mark** and then select OK.
 - To delete a number, select the number, then **Options > Delete Item**.
 - To edit a number, select the number, then **Options > Modify Item**.
 - To delete all numbers, select **Options > Delete All Items**.

To configure the whitelist

- 1 Select **Options > Settings**.
- 2 Select **Options > Antispam > Whitelist**.
- 3 Do one of the following:
 - To allow a number that is not in your contact list, select **Options > Add Item**. Type the user name and phone number, and select OK.
 - To add a number that is in your contact list, select **Options > From Phonebook**. Using the joystick, highlight the contact to add. Select **Options > Mark/Unmark > Mark** and then select OK.
 - To delete a number, select the number, then **Options > Delete Item**.
 - To edit a number, select the number, then **Options > Modify Item**.
 - To delete all numbers, select **Options > Delete All Items**.



Note: The whitelist automatically includes the numbers in your contact list.

Incoming call filter

Incoming call filter blocks calls that you are too busy to answer. You can

- block calls except for whitelisted callers, or callers in the Phonebook
- ignore calls (mute the ringer) from blocked callers
- send blocked callers the busy signal
- forward blocked calls to another number
- send blocked callers a text message
- enable blocked callers to leave a voice message

To view incoming call filter status

- 1 Do one of the following:
 - select Call
 - select **Options > Incoming Call Filter**.

The following information is displayed:

Incoming Call filter	On or Off
Action Mode	The selected mode. See Default Action setting.
Total reject calls	The number of calls rejected.
Total voice message	The number of voice messages from blocked callers.
Total unplayed voice msg	The number of new (unplayed) voice messages.

To reset rejected calls total

- Select **Options > Reset 'Total reject..**

To set the Filter Mode

The Filter Mode determines which callers the Incoming Call Filter blocks.

- 1 Select **Options > Settings > Call Manager**.

- 2 Using the joystick, set the following options:

Active Incoming Call Manager	On or Off
Scheme	Select one of the following options:
Smart filter	Reject incoming call if caller is not in the contact list or whitelist, or is in the blacklist.
Reject blacklist only	Reject call only if caller is in blacklist.
Accept whitelist only	Reject call unless caller is in whitelist.
Reject all	Block all incoming calls.
Empty Number	Select Accept or Reject. This applies to callers that do not provide their number.

To set the Default Action

The Default Action determines what happens to blocked calls.

- 1 Do one of the following:
 - If you are on the Filter Mode tab, move the joystick to the right to move to the Default Action tab.
 - Select **Options > Settings** and then select **Options > Incoming Call Filter > Default Action**.
- 2 Using the joystick, set the following options:

Default Action	Select one of the following: <ul style="list-style-type: none"> • Mute the ringer • Send busy tone • Reply by SMS • Custom diverts... • Answering machine (not available on UIQ 2.0, 2.1 and 3.0)
SMS Template	This is available if Default Action is Reply by SMS. Select the SMS message to send.
Custom Forward	This is available if Default Action is Custom Diverts. Enter the phone number for forwarded calls.
Greeting Name	If you selected Answering Machine as Default Action, select the greeting you want to play for blocked callers. To create and manage greetings, see “Working with greetings” on page 17 .
Voice Message Time	Select the maximum length for recorded messages.
Voice Message Storage	Select whether voice messages are stored in phone memory or a storage card.

To manage SMS templates

- 1 Select **Options > Settings** and then select **Options > Incoming Call Filter > SMS Templates**.
- 2 Do any of the following:
 - To add a message, select **Options > Add Item**, enter the new message and select OK.
 - To edit a message, select it with the joystick, modify it and select OK.
 - To set a message as the default, find it using the joystick and then select **Options > Set Default SMS**.
 - To delete a message, find it using the joystick and then select **Options > Delete Item**.
 - To delete all messages, select **Options > Delete All Items**.

Configuring blacklist and whitelist

You can list undesired callers in the blacklist and permitted callers in the whitelist.



Note: In both blacklist and whitelist entries, you can use wildcard characters in phone numbers. "?" replaces any single digit. "*" replaces multiple digits.

To configure the blacklist

- 1 Select **Options > Settings**.
- 2 Select **Options > Incoming Call Filter > Blacklist**.
- 3 Do one of the following:
 - To block a number, select **Options > Add Item**. Type the unwanted user name and phone number, and select OK.
 - To block a number that is in your contact list, select **Options > From Phonebook**. Using the joystick, highlight the contact to block. Select **Options > Mark/Unmark > Mark** and then select OK.
 - To delete a number, select the number, then **Options > Delete Item**.
 - To edit a number, select the number, then **Options > Modify Item**.
 - To delete all numbers, select **Options > Delete All Items**.

To configure the whitelist

- 1 Select **Options > Settings**.
- 2 Select **Options > Incoming Call Filter > Whitelist**.
- 3 Do one of the following:
 - To allow a number that is not in your contact list, select **Options > Add Item**. Type the user name and phone number, and select OK.
 - To add a number that is in your contact list, select **Options > From Phonebook**. Using the joystick, highlight the contact to add. Select **Options > Mark/Unmark > Mark** and then select OK.
 - To delete a number, select the number, then **Options > Delete Item**.
 - To edit a number, select the number, then **Options > Modify Item**.
 - To delete all numbers, select **Options > Delete All Items**.



Note: The whitelist automatically includes the numbers in your contact list.

Working with greetings

If you select the Answering Machine mode, you need to record or import at least one greeting. You can also review your greetings, select which one is the default, rename or delete greetings.



Note: Greeting feature is not available on UIQ 2.0, 2.1 and 3.0 devices.

To record a greeting

- 1 Select **Options > Settings**.
- 2 Select **Options > Incoming Call Filter > Greeting**.
- 3 Select **Options > Record**.
- 4 Enter a name for the greeting.
- 5 Select OK.
- 6 Speak your greeting and select Back when finished.

To import a greeting

- 1 Select **Options > Settings**.
- 2 Select **Options > Incoming Call Filter > Greeting**.
- 3 Select **Options > Import**.
- 4 Select the sound file to use as a greeting and then select OK.



Note: For the Import option, greetings must be .amr files saved in the Sounds directory.

To manage greetings

- 1 Select **Options > Settings**.
- 2 Select **Options > Set Default Greeting**.
- 3 Select a greeting.
- 4 From the Options menu, select one of the following actions:
 - Set default greeting - make this greeting the default one. The greeting plays.
 - Record - record a new greeting. See [“To record a greeting” on page 17](#).
 - Play - listen to the greeting
 - Rename - change greeting name
 - Delete - delete this greeting
 - Delete All - delete all greetings
 - Import - import a greeting file. See [“To import a greeting” on page 17](#).

Firewall

You can enable firewall and set the protection level on your mobile device.



Note: Firewall feature is not supported on UIQ 2.0, 2.1 and 3.0 devices.

Use FortiClient firewall to control your Internet, such as HTTP and HTTPS, and email traffic. Depending on the protection level you set, the firewall controls the inbound and outbound traffic to and from your mobile device.

The protection levels include:

- Low: The firewall allows inbound and outbound traffic.
- Medium: The firewall allows outbound traffic, but denies inbound traffic.
- High: The firewall allows common outbound traffic, but denies inbound traffic.

The common outbound traffic ports allowed include:

TCP: HTTP(80, 8080), ECHO(7), DISCARD(9), SYSTAT(11), DAYTIME(13), NETSTAT(15), FTP(21), TELNET(23), SMTP(25), WHOIS(43), TIMESERVER(42), NAMESERVER(42)

UDP: TFTP(69), FINGER(79), DNS(53)

To enable firewall and set the protection level

- 1 Select **Options > Settings > Firewall**.
- 2 Select Active Firewall and set it to On using the joystick.
- 3 Select Protection Level and set it to Low, Medium or High using the joystick.

Logs

The FortiClient program logs events such as activities performed with the program, virus detections, spam detections, and firewall detections. You can view or delete the logs.

To manage logs

- 1 Select **Options > View Log > Active log / Virus log / Call Log / Spam log / Firewall log**.
- 2 Do one of the following:
 - To see the details of a log entry, select the log, then **Options > Show Details**.
 - To delete a log entry, select the log, then **Options > Delete Item**.
 - To delete all log entries, select **Options > Delete All Items**.

Quarantine

The FortiClient program quarantines the detected virus-affected files in a special folder. You can view and manage the quarantined files.

You can set the quarantine size in 500KB increments. When the total size of quarantined files exceeds the setting, FortiClient deletes the oldest quarantined files automatically.

To view and manage the virus affected files

- 1 Select **Options > Quarantine**.
The quarantined virus affected files appear.
- 2 Select a file and do one of the following:
 - To view the file, select **Options > Show Details**.
 - To send a file to where it was from, select **Options > Recover**.
 - To send a file to a place you want, select **Options > Recover to**. Select the destination.
 - To delete the file, select **Options > Delete Item**.
- 3 To delete all files in the folder, select **Options > Delete All Items**.



Note: The "Recover to" option is not available on UIQ 3.0 devices.

To configure quarantine settings

- 1 Select **Options > Settings**.
- 2 Select **Options > Antivirus > Quarantine Settings**.
- 3 Using the joystick, set the following options:

Active Quarantine	Set to On or Off.
Quarantine Size	With the joystick, select and move the slider to the desired size of quarantine space, then select again.

Viewing version number

You can view the FortiClient program version number and copyright information by selecting **Options > About**.

Index

A

- answering machine
 - incoming call filter 14
- antispam 12
- Antivirus 10
- antivirus
 - settings 10
 - update 11
- antivirus scan
 - for a specified directory 10
 - manual 10
 - scheduling 10
- AV engine and signature
 - update 11
 - viewing version number 19

B

- Bill prompt 11
- blacklist
 - antispam, configuring 12
- blacklist, antispam
 - configuring 12
- blacklist, call filter
 - configuring 16

C

- comments on Fortinet technical documentation 5
- customer service and technical support 6

D

- default action, incoming call filter 14

F

- filter mode, incoming call filter 13
- firewall 18
- FortiClient window, accessing 9
- FortiTray 9

G

- greeting name
 - incoming call filter 14
- greetings, incoming call filter
 - importing 17
 - managing 17
 - recording 17

H

- hardware platforms
 - supported 7

I

- incoming call filter 13
 - answering machine 14
 - call forward 14
 - default action 14
 - divert call 14
 - filter mode 13
 - greetings 17
 - SMS reply 14
 - viewing status 13
- installation 7

K

- Knowledge Center 5

L

- license renew prompt, enabling 11
- Logs 18
- logs
 - managing 18

Q

- quarantine 19

R

- real-time protection, enabling 10
- rejected calls total, resetting 13

S

- scan
 - Antivirus 10
- SMS antispam 12
 - enabling 12
 - view log 12
- SMS messages
 - discarding rejected 12
- SMS Template
 - incoming call filter 14
- status
 - FortiTray indicators 9
 - incoming call filter 13
- Symbian OS versions
 - supported 7

T

- total rejected calls
 - resetting 13

U

- update, antivirus
 - scheduling updates 11
 - setting connection for updates 11
 - starting manually 11

V

- version number
 - viewing 19
- voice message storage
 - incoming call filter 14

- voice message time
 - incoming call filter 14

W

- whitelist
 - antispam, configuring 12
- whitelist, antispam
 - configuring 13
- whitelist, call filter
 - configuring 16