



**FortiClient Host Security for Symbian OS
Version 4.0**

FORTINET™

www.fortinet.com

FortiClient Host Security for Symbian OS User Guide
Version 4.0
February 19, 2008
04-40000-0251-20080219

© Copyright 2008 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
Quick access to FortiClient application	9
FortiClient console	10
Viewing version number	12
System settings	12
FortiClient Trayicon	13
To enable or disable Trayicons.....	13
Logs	13
To manage logs.....	13
Scan (Antivirus)	14
To launch a manual AV scan of all files on the mobile device.....	14
To scan files in a specified directory.....	14
To set an AV scan schedule	14
To enable real-time protection	14
To change Antivirus settings.....	14
Quarantine.....	15
To view and manage the virus affected files.....	15
To configure quarantine settings	15
Incoming call filter	16
To view incoming call filter status	16
To reset rejected calls total.....	16
Changing call filter settings	16
To set Call Filter mode.....	17
To set the Default Action	17
Working with SMS reply messages.....	18
To manage SMS reply messages.....	18

Configuring call filter blacklist and whitelist.....	18
To configure the blacklist or whitelist.....	18
Working with greetings.....	19
To record a greeting	19
To import a greeting	19
To manage greetings.....	19
SMS Antispam	20
To enable SMS Filter features.....	20
To view the Spam log	20
Configuring SMS blacklist and whitelist	20
To configure the blacklist or whitelist.....	20
Firewall	21
To enable firewall and set the protection level	21
Encryption (Phone security).....	22
To enable or disable encryption	22
Encryption settings.....	22
To change encryption settings.....	22
Encrypting contacts.....	22
To encrypt contacts	22
Working with encrypted contacts	23
To view or call encrypted contacts	23
Working with encrypted SMS messages	23
To access encrypted SMS messages	23
Working with Encrypted event logs (Call Record).....	23
To access encrypted call records	23
Using the encrypted notepad	24
To use the encrypted notepad.....	24
Working with encrypted files	24
To work with encrypted files	24
Update	25
To initiate an immediate update	25
To select the connection for updates.....	25
To enable or disable the license renewal warning.....	25
To set an update schedule	25
Index.....	27

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.
- Incoming Call Filter -- blocks calls that you are too busy to answer. You can send blocked callers an SMS message or enable them to leave a message.
- SMS antispam -- blocks unwanted SMS messages and optionally blocks WAP push messages.
- Firewall protection -- protects your Internet, such as HTTP and HTTPS, and email traffic. (Not available on Symbian OS 9.0.)
- Phone Security -- encrypts your contacts and personal information to secure your data in case your phone is lost or stolen.
- 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:

- all

Symbian UIQ OS 2.0/2.1:

- Sony Ericsson P910c, Nokia 6708

Symbian UIQ OS 3.0:

- Sony Ericsson M608 and P990i

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:

- [Quick access to FortiClient application](#)
- [FortiClient console](#)
- [Viewing version number](#)
- [System settings](#)
- [Logs](#)
- [Scan \(Antivirus\)](#)
- [Quarantine](#)
- [Incoming call filter](#)
- [SMS Antispam](#)
- [Firewall](#)
- [Encryption \(Phone security\)](#)
- [Update](#)

Quick access to FortiClient application

You can access the FortiClient application at any time, even while using another application. Press the Edit key and * at the same time. The pop-up Shortcuts menu provides access as follows:

Console	Enters the main menu of the FortiClient application. Select Exit when finished.
Encrypt Console	Enters the Encrypt menu of the FortiClient application. Select Exit when finished.
Encrypt	Encrypts your currently unencrypted data. Exits when finished.
Decrypt	Decrypts your encrypted data. Exits when finished.


After the FortiClient application exits, the device returns to the previous application.













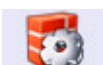
You can change the hotkey (default Edit + *) in **Help&Support > System Settings**.








FortiClient console

When you start the FortiClient application from the Start menu or open the FortiClient Console from the FortiTray, you see the FortiClient main menu. Each icon represents a program feature, and in most cases if you tap the icon you see the menu for the functions within the feature.

The table below shows the features and functions that you can access through the FortiClient main menu.

Help&Support		
	Help	View online Help.
	System log	View and clear system event logs. See “Logs” on page 13.
	System settings	Configure general system options. See “System settings” on page 12.
	Register	Register your FortiClient application.
	About	View information about this release of FortiClient for Symbian.
Scan (Antivirus)		
	Real-time Protection	Tap icon to turn Real-time Protection on or off. Real-time Monitor scans files whenever they are opened.
	Full Scan	Scan the file system of your device for viruses. See “Scan (Antivirus)” on page 14.
	Custom Scan	Scan a selected folder in your device file system. See “Scan (Antivirus)” on page 14.
	Quarantine	View the list of quarantined files. Restore or delete quarantined files. See “Quarantine” on page 15.
	Virus Log	View and clear antivirus logs. See “Logs” on page 13.
	Settings	Go to Antivirus settings. See “Scan (Antivirus)” on page 14.

	Call Filter (Incoming Call Manager)	
	Call Filter	Tap icon to turn call filter on or off. For more information, see “Incoming call filter” on page 16.
	Call log	View and clear call manager logs. See “Logs” on page 13.
	Voice Message	View, hear and delete your messages.
	Greeting	Manage voice greeting files. See “Working with greetings” on page 19.
	Settings	See “Changing call filter settings” on page 16.
	SMS Filter (Antispam)	
	SMS Filter	Tap to turn antispam monitoring on or off.
	Spam log	View and clear antispam logs. See “Logs” on page 13.
	Settings	Select to set SMS Antispam filter options. For more information, see “SMS Antispam” on page 20.
	Firewall	
	Firewall	Tap to turn monitor on or off.
	Firewall Log	View and clear firewall logs. See “Logs” on page 13.
	Settings	Set Firewall protection to Low, Normal or High. For more information, see “Firewall” on page 21.

	Phone security	Use data encryption. You can encrypt contacts, SMS messages, call log, files and notes. See "Encryption (Phone security)" on page 22.
	Phone security	Tap to encrypt or decrypt personal data. Lower part of screen shows current status.
	Browse Encrypted Contacts	View the encrypted contacts list. See "Encrypting contacts" on page 22 and "Working with encrypted contacts" on page 23.
	Browse Encrypted Messages	View encrypted SMS messages. See "Working with encrypted SMS messages" on page 23.
	Encrypted Event Logs	View and clear phone logs. See "Logs" on page 13.
	File Encryption	Encrypt files. Back up or restore encrypted files. See "Working with encrypted files" on page 24.
	Notepad	Keep encrypted notes. See "Using the encrypted notepad" on page 24.
	Settings	See "Encryption settings" on page 22.
	Update	Update your Antivirus database. See "Update" on page 25.

Viewing version number

You can view the FortiClient program version number and copyright information by selecting **Help&Support > About** from the FortiClient main menu.

System settings

Select **Help&Support > System Settings** to configure several options that affect all operations:





Display TrayIcon	Select On to provide indication of FortiClient application status at all times. See "FortiClient Trayicon" on page 13.
Enable sound	Select On to enable audio alert when a virus is found.
Default connection	Select the default Internet connection. select the default connection. If you do not always use the same connection, select Always Ask.
Internet Bill Prompt	Select On to have your phone ask permission before connecting to the Internet.

Dial Bill Prompt	Select On to have your phone ask permission before dialing a phone number.
Send SMS Bill Prompt	Select On to have your phone ask permission before sending an SMS message.
Hotkey	Enter a new hotkey combination. The default is Edit + *. The hotkey provides access to the FortiClient application at any time. See "Quick access to FortiClient application" on page 9 .

FortiClient Trayicon

If Display Trayicon 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 Trayicons

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

To enable or disable Trayicons

- 1 Start the FortiClient application.
- 2 Select **Help&Support > System Settings**.
- 3 With the joystick, set Display Trayicon On or Off.

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 From the FortiClient main menu, select **Help&Support > System Log**.
- 2 Move the joystick right or left to select the tab for the type of log: Activity, Virus, Call, Spam, Firewall.
- 3 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**.

Scan (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 14](#)).

If Quarantine is enabled (see [“Quarantine” on page 15](#)), 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 From the FortiClient main menu, select **Scan > Full Scan**.
The scanning process starts. When it completes, 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 From the FortiClient main menu, select **Scan > Custom Scan**.
- 2 Navigate to the directory that you want to scan, using the joystick.
- 3 Select OK.

The scanning process starts. When it completes, the scanning result appears.

To set an AV scan schedule

- 1 From the FortiClient main menu, select **Scan > Settings**.
- 2 Move the joystick to the right to select the Schedule Scan tab.
- 3 Set the Scan Frequency and options to one of the following:
 - Manual (no scheduled scans)
 - Daily + Start Time
 - Weekly + Start Time + Day
 - Monthly + Start Time + Date

The schedule is activated when you exit the application.

To enable real-time protection

- 1 From the FortiClient main menu, select **Scan**.
- 2 Select **Real-time Protection** to toggle feature on or off.

To change Antivirus settings

- 1 Select **Scan > 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

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 From the FortiClient main menu, select **Scan > Quarantine**.
- 2 Select a file and do one of the following:
 - To view the file, select **Options > Show Details**.
 - To restore a file to its original location, select **Options > Recover**.
 - To restore a file to a different location, 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 From the FortiClient main menu, select **Scan > Settings**.
- 2 Move the joystick to the right to select the Quarantine Settings tab.
- 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.

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 Contacts
- 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 From the FortiClient main menu, select Call Filter with the joystick.
If Call Filter is enabled, the Call Filter icon includes a green checkmark and the following information is displayed:

Scheme	The selected mode. See Scheme in settings.
Action Mode	The selected action on blocked calls. See Default Action.

- 2 Using the joystick, highlight the Call Log icon. View the following information in the lower portion of the screen:

Total rejected	The total number of calls rejected.
Today	The number of calls rejected today.
Recent phone	The phone number of the most recent blocked call.
Recent date	The date of the most recent blocked call.

- 3 Using the joystick, highlight the Voice Message icon. The lower portion of the screen shows the number of voice messages in total (Sum) and the number of unread (New) voice messages.

To reset rejected calls total

- 1 From the FortiClient main menu, select **Call Filter**.
- 2 Select **Options > Reset Total Rejected**.

Changing call filter settings

To modify all call filter settings, select **Call Filter > Settings** from the main FortiClient menu. The settings page is divided into tabs:

Filter mode	determines which callers are blocked
Default Action	determines how to respond to a blocked caller
White List	lists callers who should not be blocked
Black List	lists callers who should always be blocked
SMS Templates	contains SMS reply messages for use with Reply by SMS action
Greeting	contains voice greetings for Answering Machine action

You can move from tab to tab by moving the joystick right or left.

To set Call Filter mode

- 1 From the FortiClient main menu, select **Call Filter > Settings**.

You are viewing the Filter Mode tab.

- 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 From the FortiClient main menu, select **Call Filter > Settings**.
- 2 Using the joystick, select the Default Action tab.
- 3 Using the joystick, set the following options:

Default Action	Select how the Call Filter responds to blocked callers:
Mute the ringer	Ignore incoming call.
Send busy tone	Send busy signal to blocked caller.
Reply by SMS	Send SMS reply message to blocked caller. Select the message in the SMS Template option.
Answering machine	Play a recorded greeting and ask the caller to leave a voice message. Select the recorded greeting in the Greeting Name option and adjust Voice Message Time and Voice Message Storage options as needed. This feature is not available on UIQ 2.0, 2.1 and 3.0 phones.
Custom diverts...	Forward the call to another phone number. Select the forwarding destination in the Custom Forward option.

The Default Action you select determines which of the following options are available.

SMS Template	You selected Reply by SMS as Default Action. Select the SMS reply message to send. To create and manage SMS reply messages, see "Working with SMS reply messages" on page 18 .
Custom Forward	You selected Custom Diverts as Default Action. Enter the phone number for forwarded calls.
Greeting Name	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 19 .
Voice Message Time	You selected Answering Machine as Default Action. Select the maximum length for recorded messages.
Voice Message Storage	You selected Answering Machine as Default Action. Select whether voice messages are stored in phone memory or on a storage card.

Working with SMS reply messages

If you selected Reply by SMS as the call filter default action, you need to select an SMS reply message to send. If the pre-programmed messages are not appropriate, you can modify them, delete them or create your own messages.

To manage SMS reply messages

- 1 From the FortiClient main menu, select **Call Filter > Settings**.
- 2 Using the joystick, select the SMS Templates tab.
- 3 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 call filter 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 or whitelist

- 1 From the FortiClient main menu, select **Call Filter > Settings**.
- 2 Using the joystick, select the Black List or White List tab as needed.
- 3 Do one of the following:
 - To add a number, select **Options > Add Item**. Enter the caller name and phone number, and select OK.
 - To add a number that is in your contact list, select **Options > From Contacts**. Using the joystick, highlight the contact to add. Press the joystick or 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 selected Answering Machine as the call filter default action, 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 From the FortiClient main menu, select **Call Filter > Greeting**.
- 2 Select **Options > Record**.
- 3 Enter a name for the greeting.
- 4 Select OK.
- 5 Speak your greeting and select Back when finished.

To import a greeting

- 1 From the FortiClient main menu, select **Call Filter > Greeting**.
- 2 Select **Options > Import**.
- 3 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 From the FortiClient main menu, select **Call Filter > Greeting**.
- 2 Select a greeting.
- 3 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 19](#).
 - 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 19](#).

SMS 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.

The FortiClient program applies antispam rules in the following order:

- block unidentified caller (empty number)
- allow whitelisted caller
- block blacklisted caller
- block caller not in contact list (unknown number)

To enable SMS Filter features

- 1 From the FortiClient main menu, select **SMS Filter > Settings**.
- 2 Using the joystick, set the following options:

Active SMS Filter	Set On to block unwanted SMS messages, otherwise set Off.
Filter WAP Push Msgs	Set On to also block WAP Push Msgs.
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 From the FortiClient main menu, select **SMS Filter > Spam log**.

Configuring SMS 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 or whitelist

- 1 From the FortiClient main menu, select **SMS Filter > Settings**.
- 2 Using the joystick, select the Black List or White List tab as needed.

- 3 Do one of the following:
 - To add a number, select **Options > Add Item**. Type the caller name and phone number, and select OK.
 - To add a number that is in your contact list, select **Options > From Contacts**. Using the joystick, highlight the contact. Press the joystick or 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.

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, 3.0 and Symbian OS 9.0 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 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 From the FortiClient main menu, select **Firewall> Settings**.
- 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.

Encryption (Phone security)

The FortiClient program can encrypt your contacts and personal information. This secures your data in case your phone is lost or stolen.

To access encryption functions, select Phone security from the FortiClient main menu. The first time you do this, FortiClient asks you to set a password. You must use this password every time you enter the Phone security menu.

For quick access to the encryption functions at any time, press the Edit key and * at the same time and then select Encrypt Console from the menu.

To enable or disable encryption

- 1 Select **Phone security** and enter your password.
- 2 Select **Phone security**.

When encryption is enabled, the **Phone security** icon includes a green check mark.

Encryption settings

To change encryption settings

- 1 Select **Phone security** and enter your password.
- 2 Ensure that encryption is off.
- 3 Select **Settings**.
- 4 Using the joystick, set the following options:

Password	Change your password. Enter new password and select OK.
Reboot auto encrypt	Select On to encrypt data when the phone is restarted.
Encrypt store	Select Phone Memory or Storage Card for encrypted file storage.
Auto encrypt on idle	Select On to encrypt data when the phone is idle.
Decryption range	Select to decrypt all messages or only messages that arrived: <ul style="list-style-type: none"> • within one day • within one week • within one month

Encrypting contacts

The contacts that you want to encrypt must belong to a group. See the Symbian documentation for more information about contacts and contact groups.

To encrypt contacts

- 1 Select **Phone security** and enter your password.
- 2 Ensure that encryption is off.
- 3 Select **Settings**.
- 4 Move the joystick to the right to select the Add/Remove Group tab.
Your contact groups are listed.
- 5 Select the group that you want to add and press the joystick.

When the group is selected for encryption, the icon shows a key.

- 6 Select **Back**.
- 7 Select **Phone security**.
The group(s) of contacts that you selected are encrypted. They no longer appear in the standard Contacts list.

Working with encrypted contacts

Encrypted contacts are not visible in the standard Contacts list. You must access them through the Phone security function.

To view or call encrypted contacts

- 1 Select **Phone security** and enter your password.
- 2 Ensure that encryption is on.
- 3 Select **Browse encrypted contacts**.
Using the Options menu, you can view contact details, send SMS to, phone or decrypt the contact.

Working with encrypted SMS messages

When encryption is on, you can view encrypted SMS messages in the Encrypted SMS Page. You can also restore (decrypt) messages to the normal SMS message inbox.

To access encrypted SMS messages

- 1 Select **Phone security** and enter your password.
- 2 Ensure that encryption is on.
- 3 Select **Browse encrypted messages**.
- 4 Do any of the following:
 - To view a message, select the message and then select **Options > Show Details**.
 - To view the status of all encrypted SMS messages, select **Options > Summary**.
 - To restore (decrypt) a message to the normal SMS Inbox, select the message and then select **Options > Restore**.
 - To delete a message, select the message and then select **Options > Delete item**.
 - To delete all encrypted messages, select **Options > Delete all items**.

Working with Encrypted event logs (Call Record)

When encryption is on, you can check encrypted call records in the Encrypted logs page.

To access encrypted call records

- 1 Select **Phone security** and enter your password.
- 2 Ensure that encryption is on.
- 3 Select Encrypted Event Logs.

- 4 Do any of the following:
 - To view call details, select the call record and then select **Options > Show Details**.
 - To send an SMS Message to an encrypted contact, select the call record and then select **Options > Send SMS to this**.
 - To call an encrypted contact, select the call record and then select **Options > Dial this**.
 - To delete an encrypted call record, Select the call record and then select **Options > Delete item**.
 - To delete all encrypted call records, select **Options > Delete all items**.

Using the encrypted notepad

You can keep confidential notes in the encrypted notepad.

To use the encrypted notepad

- 1 Select **Phone security** and enter your password.
- 2 Ensure that encryption is on.
- 3 Select Notepad.
- 4 Do any one the following:
 - To add a new note, select **Options > Add**, write the note and select OK.
 - To edit an existing note, select the note and then select **Options > Open**. Select OK when you are finished editing.
 - To delete a note, select the note and then select **Options > Delete**.

Working with encrypted files

You can encrypt files to keep them confidential.

To work with encrypted files

- 1 Select **Phone security** and enter your password.
- 2 Ensure that encryption is on.
- 3 Select **File Encryption**.
- 4 Do any of the following:
 - To encrypt a file, select **Options > Add File**, find the file and then select OK. If you want to delete the original file, select Yes. Otherwise select No.
 - To write a memo for a file, select the file and then select **Options > Write Memo**. Enter the memo text and then select OK.
 - To rename an encrypted file, select the file and then select **Options > Rename**. Edit the file name and then select OK.
 - To back up an encrypted file, select the file and then select **Options > Backup**. Select where to save the file and then select OK.
 - To restore an encrypted file from a backup file, select **Options > Restore**, use the joystick to find the backup file and then select OK. Enter your password and select OK.

- To extract an encrypted file to another location, select the file and then select **Options > Extract**. Use the joystick to select where to save the file and then select OK.
- To delete all encrypted files, select **Options > Format**. Select Yes to confirm that you want to delete the files.

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

To initiate an immediate update

- 1 From the FortiClient main menu, select **Update**.
 - 2 If asked, select the access point.
- The update status bar displays the update progress.



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

To select the connection for updates

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

To enable or disable the license renewal warning

- 1 Select **Help&Support > System Settings**.
- 2 Set Internet Bill Prompt to On or Off using the joystick.

To set an update schedule

- 1 Select **Help&Support > System Settings**
- 2 Move the joystick to the right to select the Schedule Update tab.
- 3 Set the Update Frequency and options to one of the following:
 - Never
 - Daily + Start Time
 - Weekly + Start Time + Day
 - Monthly + Start Time + Date

The schedule is activated when you exit the application.

Index

A

- answering machine
 - incoming call filter 17
- antispam 20
- Antivirus 14
- antivirus
 - settings 14
 - update 25
- antivirus scan
 - for a specified directory 14
 - manual 14
 - scheduling 14
- AV engine and signature
 - update 25
 - viewing version number 12

B

- bill prompt 25
 - dial 13
 - network 12
 - SMS 13
- blacklist
 - antispam, configuring 20
- blacklist, antispam
 - configuring 20
- blacklist, call filter
 - configuring 18

C

- call records
 - encrypted 23
- comments on Fortinet technical documentation 5
- contacts
 - encrypting 22
 - working with encrypted 23
- customer service and technical support 6

D

- default action, incoming call filter 17
- dial bill prompt 13

E

- encryption 22
- event logs
 - encrypted 23

F

- filter mode, incoming call filter 17
- firewall 21
- FortiTray 13

G

- greeting name
 - incoming call filter 17
- greetings, incoming call filter
 - importing 19
 - managing 19
 - recording 19

H

- hardware platforms
 - supported 7

I

- incoming call filter 16
 - answering machine 17
 - call forward 17
 - default action 17
 - divert call 17
 - filter mode 17
 - greetings 19
 - SMS reply 17
 - viewing status 16
- installation 7

K

- Knowledge Center 5

L

- license renew prompt, enabling 25
- Logs 13
- logs
 - managing 13

N

- network bill prompt 12
- notepad
 - encrypted 24

P

- phone security 22
 - encrypted event logs 23
 - encrypted files 24
 - encrypted notepad 24
 - encrypting contacts 22
 - encrypting SMS messages 23
 - settings 22

Q

- quarantine 15

R

real-time protection, enabling 14
rejected calls total, resetting 16

S

scan
 Antivirus 14
SMS antispam 20
 enabling 20
 view log 20
SMS bill prompt 13
SMS messages
 discarding rejected 20
 encrypting 23
SMS Template
 incoming call filter 17
status
 FortiTray indicators 13
 incoming call filter 16
Symbian OS versions
 supported 7

T

total rejected calls
 resetting 16

U

update, antivirus
 scheduling updates 25
 setting connection for updates 25
 starting manually 25

V

version number
 viewing 12
voice message storage
 incoming call filter 17
voice message time
 incoming call filter 17

W

WAP push message
 filtering 20
whitelist
 antispam, configuring 20
whitelist, antispam
 configuring 20
whitelist, call filter
 configuring 18

FORTINET™

www.fortinet.com

FORTINET™

www.fortinet.com