

FortiClient Host Security for Windows Mobile Version 4.0

FORTINET™

www.fortinet.com

FortiClient Host Security for Windows Mobile User Guide
Version 4.0
November 8, 2007
04-40000-0247-20071108

© 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

ABACAS, APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, 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

Installation	5
Supported hardware and software platforms	5
Installing the FortiClient program	5
To install from the FortiClient CAB file	5
Starting the FortiClient program	5
Configuration.....	7
FortiTray	7
FortiClient console	8
Antivirus	11
Setting Antivirus options.....	11
Scanning files.....	12
To launch a manual AV scan.....	12
Working with quarantined files	13
Incoming call filter	14
Viewing Call Filter status.....	14
Setting Call Filter options	15
Working with lists	15
To add an entry to the list	16
To edit an entry in the list.....	16
To add an entry from your contact list	16
To delete an entry from the list	16
SMS Antispam.....	17
Setting Antispam options	17
To manage the WhiteList/BlackList	17
VPN	18
To configure a VPN tunnel.....	18
To connect to a VPN.....	18
To disconnect from a VPN.....	18
To manually update VPN tunnel status	18
To modify a VPN tunnel.....	19
To delete a VPN tunnel.....	19
Phone Security.....	19
Working with encrypted files	20
To add a file	20
To delete a file	20
To decrypt a file to a new location	20
To view information about a file	20
To add memo information to a file	20
To back up all encrypted files	20
To restore all encrypted files.....	20
To destroy all encrypted files	20

Using Safe Notebook	21
To add a note	21
To delete a note.....	21
To open a note to read or edit	21
Setting Security Options	22
Changing your password	23
To change your password	23
To set up password protection (password recovery).....	23
To recover a lost password	23
Update	24
To initiate an immediate update	24
System Options	25
To configure automatic updates or antivirus scans	25
Logs	26
To view and manage logs.....	26
Index.....	27

Installation

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

The following topics are included in this section:

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

Supported hardware and software platforms

All pocket PC PDAs and smart phones with Windows Mobile 2003 Second Edition operating system.

Installing the FortiClient program

There are two ways to install the FortiClient program onto your mobile devices:

- Install from a PC with MS ActiveSync. For information on how to use ActiveSync, see ActiveSync online help.
- Install from the FortiClient CAB file.

To install from the FortiClient CAB file

- 1 Download the FortiClient CAB file to your PC.
- 2 Connect your mobile device to your PC.
- 3 Copy the CAB file to your mobile device.
- 4 Tap the CAB file. The program will be installed.

Starting the FortiClient program

- 1 Tap Start > Programs.
- 2 Tap FortiClient.

Configuration

This section describes how to use the following FortiClient features:

- [FortiTray](#)
- [FortiClient console](#)
- [Antivirus](#)
- [Incoming call filter](#)
- [SMS Antispam](#)
- [VPN](#)
- [Phone Security](#)
- [Update](#)
- [Logs](#)

FortiTray

The FortiTray provides quick access to basic FortiClient settings and to the FortiClient console. Using the FortiClient Console, you can configure and monitor the operation of your FortiClient application.



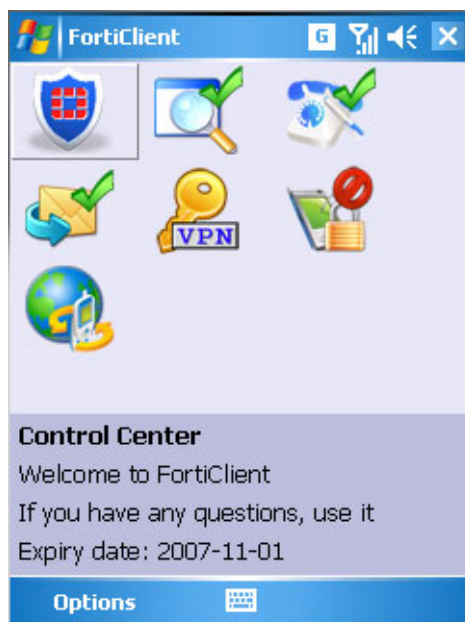
Select the FortiTray icon in the lower right corner of the Today screen to view the FortiTray menu. The FortiTray menu contains the following items:







Open FortiClient Console	Select to open the FortiClient Console at the Dashboard page, from which you can access all FortiClient settings. For more information, see “FortiClient console” on page 8 .
Disable or Enable Realtime AV Protection	Select to enable or disable Realtime AV Protection. For more information about AV protection, see “Antivirus” on page 11 .
Disable or Enable SMS Filter	Select to enable or disable the SMS Antispam filter. For more information, see “SMS Antispam” on page 17 .
Disable or Enable CallFilter	Select to enable or disable incoming call management. For more information, see “Incoming call filter” on page 14 .
Encrypt or Decrypt Data	Encrypt or access encrypted contacts, call log items, messages.

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 main menu.

Figure 1: Main menu



Control Center	
	
	System Log View and clear system event logs. See “Logs” on page 26.
	System Option Configure scheduled updates and scheduled antivirus scans. See “System Options” on page 25.
	Help View online Help.
	Register Register your FortiClient application.
	About Information about this release of FortiClient for Windows Mobile.



Antivirus



Realtime Monitor Tap icon to turn Realtime Monitor on or off. Real-time Monitor scans files whenever they are opened.



Scan File System Scan the file system of your device for viruses. See [“To launch a manual AV scan” on page 12.](#)



Quarantine View the list of quarantined files. Restore or delete quarantined files. See [“Working with quarantined files” on page 13.](#)



Antivirus Log View and clear antivirus logs. See [“Logs” on page 26.](#)



Antivirus Options Go to Antivirus settings. See [“Antivirus” on page 11.](#)



Incoming Call Manager



Callwall Monitor Tap icon to turn monitor on or off. For more information, see [“Incoming call filter” on page 14.](#)



CallWall Log View and clear call manager logs. See [“Logs” on page 26.](#)



Callwall Options See [“Setting Call Filter options” on page 15.](#)



Antispam



Antispam Monitor Tap to turn antispam monitoring on or off.



Antispam Log View and clear antispam logs. See [“Logs” on page 26.](#)











Antispam Options Select to set SMS Antispam filter options. For more information, see [“SMS Antispam” on page 17.](#)



VPN

Use a Virtual Private Network (VPN) tunnel. For more information, see [“VPN” on page 18.](#)

	Phone Security	Use data encryption. You can encrypt contacts, SMS messages, call log, files and notes. See “Phone Security” on page 19.
	Encrypt Status	Tap to encrypt or decrypt personal data. Lower part of screen shows current status.
	View Contacts	View the encrypted contacts list.
	View Encrypted SMS	View encrypted SMS messages.
	View Call Log	View and clear phone logs. See “Logs” on page 26.
	File Encrypt	Encrypt files. Back up or restore encrypted files. See “Working with encrypted files” on page 20.
	Safe Notebook	See “Using Safe Notebook” on page 21.
	Security Options	See “Setting Security Options” on page 22.
	Update	Update your Antivirus database. See “Update” on page 24.

Antivirus

The FortiClient program protects your mobile device from virus attacks. It supports both on-demand (manual) and scheduled file system scanning. You can also enable real-time file protection which scans files whenever they are opened.

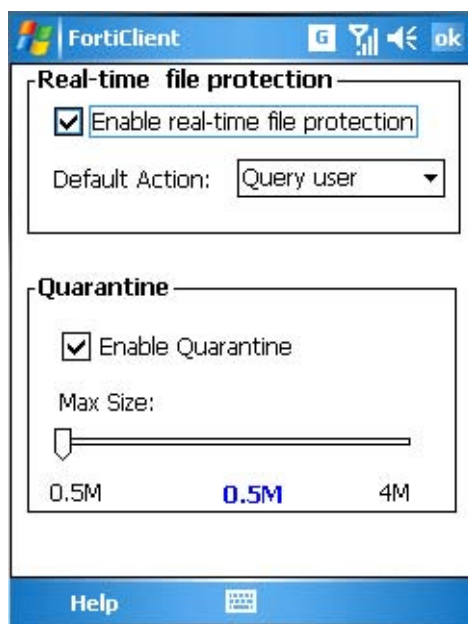
Optionally, you can quarantine files found to contain viruses. Then, you can view a list of the quarantined files and delete or restore them. For more information, see [“Working with quarantined files” on page 13](#).

Antivirus activities are logged. To view the logs, tap **Antivirus > Antivirus Log**. For more information about viewing logs, see [“Logs” on page 26](#).

Setting Antivirus options

To view or modify Antivirus settings, tap **Antivirus > Antivirus Options** on the FortiClient main menu.

Figure 2: Antivirus tab



- Enable real-time file protection** Scan each file on access.
- Default Action** If real-time protection is enabled, select one of:
 - Query user** ask user whether to delete the file
 - Delete** quarantine (if enabled) or delete the infected file
 - Ignore** take no action on the infected file
- Enable Quarantine** Send infected files to quarantine instead of deleting them.
- Max size** Select the amount of device memory to reserve for quarantined files. When the allocated space for quarantined files is full, the oldest files are deleted as needed to free space for new files.

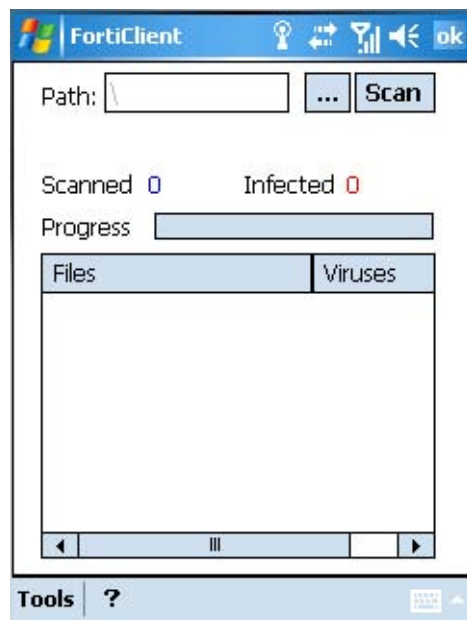
You can view quarantined files and restore them or delete them permanently. See [“Working with quarantined files” on page 13](#).

Scanning files

To scan your device file system, tap **Antivirus > Scan File System** on the FortiClient main menu.

You can also set up scheduled antivirus scanning of your file system. See [“System Options” on page 25](#).

Figure 3: Manual file system scan



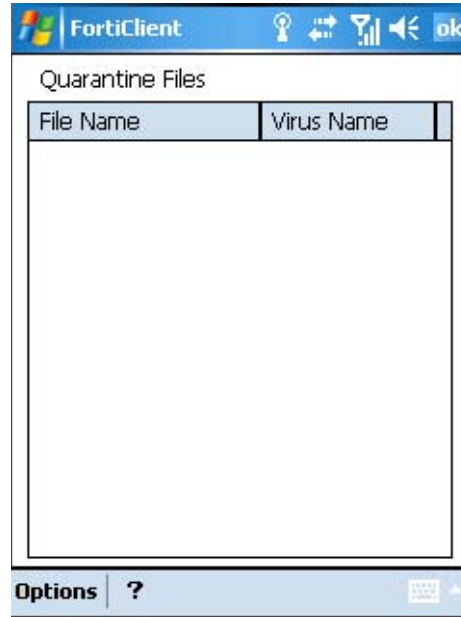
To launch a manual AV scan

- 1 Optionally, tap the ellipsis (...) button and select the path to scan. By default, the FortiClient application scans the entire device file system.
- 2 Tap the Scan button.
If desired, tap Stop at any time to stop scanning.
If any virus-infected files are found, they appear in the Infected file(s) list.
- 3 After the scan is done, tap OK.

Working with quarantined files

Tap **Antivirus > Quarantine** to view a list of your quarantined files. You can restore or delete the files.

Figure 4: Quarantine Files list



The Quarantine Files list shows the name of the virus detected in each quarantined file. Use the Options menu to see more information, restore or delete quarantined files.

Show details	Display additional information about the selected file.
Restore	Restore the selected file to its location in the device file system.
Restore all	Restore all files to their locations in the device file system.
Restore to...	Restore the selected file to a specified location.
Delete	Delete the selected file.
Clear all	Delete all quarantined files.
Quarantine status	Show quarantine size, quarantine space used, number of files.

Incoming call filter

The incoming call filter handles calls that you are too busy to answer. You can

- block calls except for whitelisted callers, or callers in the Phonebook
- forward blocked callers to another number
- send blocked calls a text message

This feature is available only on a SmartPhone or a Pocket PC with cell phone module. The device must be running Windows CE 2003.

Viewing Call Filter status

On the main menu, tap **Incoming Call Manager** to view call filter status information. From this menu you can also modify your settings.

Figure 5: Incoming call filter status



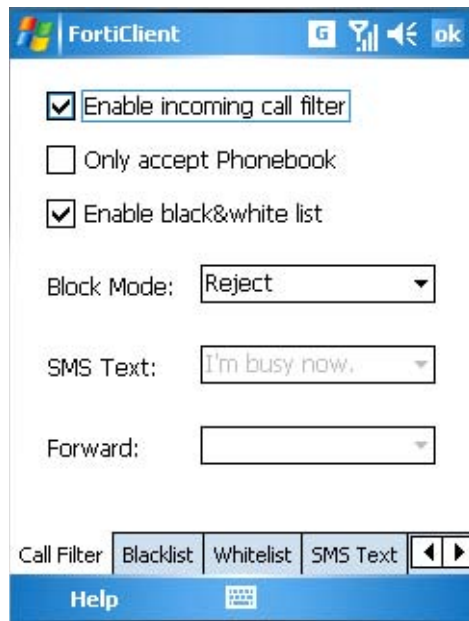
Use the joystick to highlight the icons and view information in the lower part of the screen as follows:

Callwall Monitor	Monitor status: ON or OFF
Callwall Log	Total filtered calls, total filtered calls today, phone number and time of latest filtered call. Tap icon to view log. See “Logs” on page 26 .
Callwall Options	No status information. Tap icon to change settings. See “Setting Call Filter options” on page 15 .

Setting Call Filter options

Tap **Incoming Call Manager > Callwall Options** to configure the incoming call filter.

Figure 6: Call Filter settings



- Enable incoming call filter** Select to enable call filtering.
- Only accept Phonebook** Accept calls from callers in your Phonebook, reject others.
- Enable black & white list** Enable use of blacklist and whitelist. You can configure these through the Settings menu.
- Block Mode**
 - Reject - reject the call
 - SMS Reply - send blocked caller an SMS message
 - Forward - forward calls to another number
- SMS Text** Select the text message for SMS Reply mode.
Select **Settings > SMS Text** to can create text messages.
- Forward** Select a destination for forwarded calls.
Select **Settings > Forward** to define destination numbers.

Use the tabs at the bottom of the screen to edit the Blacklist, Whitelist, SMS Text replies and Forwarding destinations. See [“Working with lists”](#).

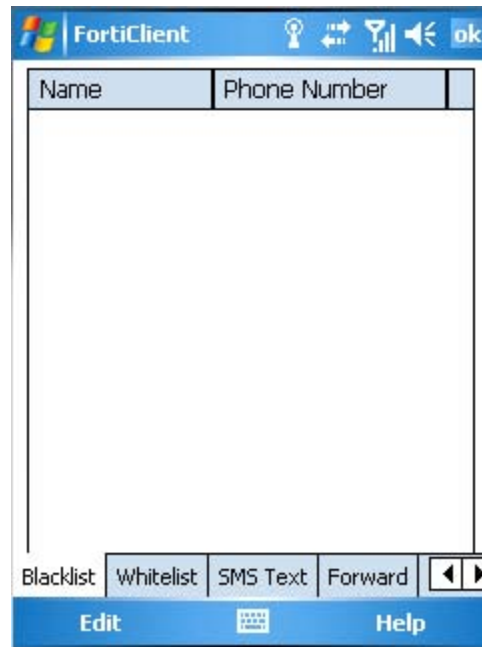
Working with lists

You can edit the following lists used in the call filter feature:

- Blacklist** Names and telephone numbers of callers to always block
- Whitelist** Names and telephone numbers of callers to always accept
- SMS Text** Text messages that can be sent to blocked callers when Block mode is SMS Reply
- Forward** Named destinations to which blocked calls can be forwarded when the Block mode is Forward

On the main menu, tap **Incoming Call Manager > Callwall Options** and then tap the tab for the list near the bottom of the screen.

Figure 7: Call management lists



To add an entry to the list

- 1 Tap **Edit > Add**.
- 2 Fill in the appropriate fields.
- 3 Select OK.

To edit an entry in the list

- 1 Tap the list entry that you want to modify.
- 2 Tap **Edit > Modify**.
- 3 Modify the information as needed.
- 4 Select OK.

To add an entry from your contact list

- 1 Tap **Edit > From Phonebook**.
- 2 Select the checkbox of each entry that you want to add.
- 3 Tap OK.

To delete an entry from the list

- 1 Tap the list entry that you want to delete.
- 2 Tap **Edit > Delete**.

SMS Antispam

Using the FortiClient program, you can block unwanted Short Message Service (SMS) messages. This feature is available only on a SmartPhone or a Pocket PC with cell phone module.

From the FortiClient main menu, tap Antispam. Tap Antispam Monitor to turn SMS Antispam on or off. Tap Antispam Log to view blocked messages.

Setting Antispam options

- 1 On the FortiClient main menu, tap **Antispam > Antispam Options**.

Figure 8: Antispam options



Enable SMS Antispam

Detect and block spam SMS messages.

Delete sms from unknown caller

Block messages from callers who are not in your contact list.

If you want to allow specific callers who are not in your contact list, add them to the White list.

Delete empty caller sms

Block messages from unidentified callers.

WhiteList

Callers to always accept.

Blacklist

Callers to always block.

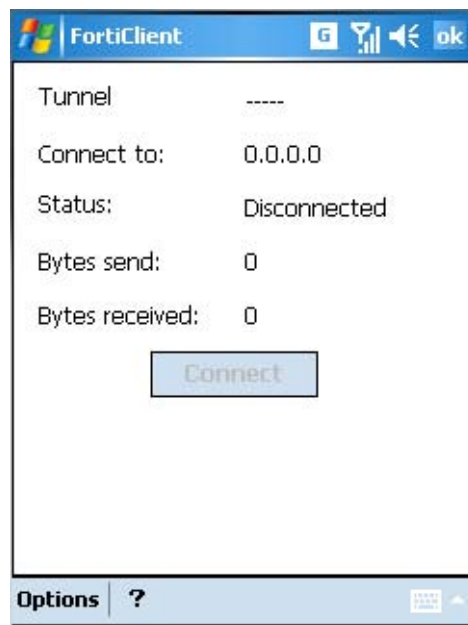
To manage the WhiteList/BlackList

- 1 On the FortiClient main menu, tap **Antispam > Antispam Options**.
- 2 Tap the WhiteList or BlackList tab, as required.
- 3 To add a number, tap Add, type the name and phone number into the appropriate fields in the Input Dialog, and then tap OK.
- 4 To delete a number, select the number and tap Del.
- 5 To delete all numbers from the list, tap Clear.

VPN

The FortiClient program can establish a virtual private network (VPN) with a FortiGate Unified Threat Management System. You create VPN configurations in FortiClient 3.0 on your PC and transfer them to your mobile device using Microsoft ActiveSync.

Figure 9: VPN page



To configure a VPN tunnel

- 1 Connect your mobile device to your PC using the USB cable.
- 2 Start Microsoft ActiveSync and make sure that it detects your device.
- 3 Create one or more VPN connections in FortiClient 3.0 on your Windows PC. For more information, refer to the FortiClient 3.0 User Guide or online Help.
- 4 On the PC, on the FortiClient VPN Connections page, select Sync to Device. Your tunnel definitions are transferred to your mobile device.

To connect to a VPN

- 1 On the FortiClient main menu, tap **VPN**.
- 2 From the Tunnel List, select the tunnel that you want to use.
- 3 Tap the Connect button.

To disconnect from a VPN

- 1 On the FortiClient main menu, tap **VPN**.
- 2 Tap the Disconnect button.

To manually update VPN tunnel status

- 1 On the FortiClient main menu, tap **VPN**.
- 2 Tap **Options > Refresh**.

To modify a VPN tunnel

You can modify only VPN tunnels that use automatic configuration.

- 1 On the FortiClient main menu, tap **VPN**.
- 2 Tap **Options > Select Tunnel**.
- 3 From the Tunnel List, select the tunnel configuration that you want to modify.
- 4 Tap **Options > Edit**.
- 5 Change the Remote Gateway address as needed.
- 6 Tap OK.

To delete a VPN tunnel

- 1 On the FortiClient main menu, tap **VPN**.
- 2 Tap **Options > Select Tunnel**.
- 3 From the Tunnel List, select the tunnel configuration that you want to remove.
- 4 Tap **Options > Delete**.

Phone Security

You can encrypt the contents of your mobile device to protect your information in case the device is lost or stolen.

To access Phone Security features, on the FortiClient main menu, tap Phone Security. Enter your password and tap OK.

The Phone Security menu contains the following items:

Encryption Status	Tap the icon to encrypt or decrypt. Security status shows in lower portion of screen: Encrypted or Decrypted. If the status is Decrypted: <ul style="list-style-type: none"> • you can access Contacts from the device main menu. • you can access Call Event Log (Call History) from the device Phone function.
View Contacts	Tap to view contacts. For details, select contact and tap Options > Show Details .
View Encrypted SMS	Tap to view messages. For details, select message and tap Operation > Detail .
View Call Log	Tap to view call log. At the top left of the window, select the type of calls to display: All Call, Missed Call, Outgoing Call, Incoming Call. To view details, select log entry and tap Options > Show Details .
File Encrypt	See “Working with encrypted files” on page 20 .
Safe Notebook	See “Using Safe Notebook” on page 21 .
Security Options	See “Setting Security Options” on page 22 .

Working with encrypted files

You can protect files on your system by encrypting them. From the main menu, tap **Phone Security > File Encrypt** to access your encrypted files.

To add a file

- 1 Tap **Edit > Add**.
- 2 Select the desired file and tap OK.
- 3 Optionally, tap **Edit > Write Memo** to make a note about the file.

To delete a file

- 1 Select the file you want to delete.
- 2 Tap **Edit > Delete**.
- 3 Tap Yes to confirm deletion.

To decrypt a file to a new location

- 1 Select the desired file.
- 2 Tap **Edit > Extract**.
- 3 Select the location to place the extracted file and tap OK.

To view information about a file

- 1 Select the desired file.
- 2 Tap **Edit > Detail**.
The file name, size, memo, and time last modified are displayed.
- 3 Tap OK.

To add memo information to a file

- 1 Select the desired file.
- 2 Tap **Edit > Write Memo**.
- 3 Enter the memo information and tap OK.

To back up all encrypted files

- 1 Tap **Edit > Backup**.
- 2 Select the location to store the backup file and tap OK.
The file name is "efsys", followed by the date and time the file was created.

To restore all encrypted files

- 1 Tap **Edit > Restore**.
- 2 In the upper part of the screen, select the location where the backup file is stored.
- 3 In the lower part of the screen, select the backup file and tap OK.
- 4 Enter the password used to encrypt the files and tap OK.

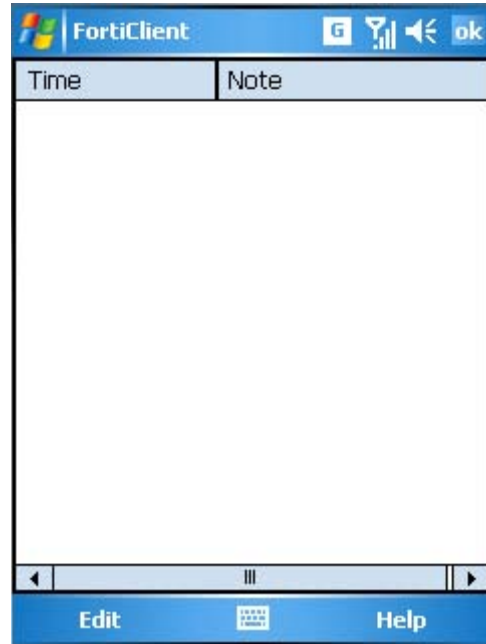
To destroy all encrypted files

- 1 Tap **Edit > Format**.
- 2 Tap Yes to destroy all encrypted files.

Using Safe Notebook

The Safe Notebook enables you to keep private notes in an encrypted notebook. On the main menu, tap **Phone Security > Safe Notebook**.

Figure 10: Safe notebook



To add a note

- 1 Tap **Edit > Add**.
- 2 Enter the note text and tap OK.

To delete a note

- 1 Select the note you want to delete.
- 2 Tap **Edit > Delete**.
- 3 Tap Yes to confirm deletion.

To open a note to read or edit

- 1 Select the note you want to read or edit.
- 2 Tap **Edit > Open**.
- 3 When you have finished, tap OK.

Setting Security Options

On the FortiClient main menu, tap **Phone Security > Security Options** to change your password.

Figure 11: Phone security options



Change Password

Select to change your password. You can also set a reminder question to help you remember your password. See [“Changing your password” on page 23](#).

Notify if received a secret SMS

If encryption is enabled, FortiClient notifies you when it receives and encrypts an SMS message.

Auto Lock

Automatically encrypt data when device is idle.

Encrypt File Driver

Select where to store encrypted files: device memory or storage card.

Decrypt SMS Received in:

Select which messages to decrypt, by time of arrival: Today, Last 7 days, Last 30 days, Any Time.

Contacts Group

Select which categories of contacts to encrypt. Contacts not assigned to one of these groups are not encrypted.

Changing your password

You can change your password and set a question for password recovery. From the Phone Security menu, tap **Security Options > Change Password**.

Figure 12: Change password

To change your password

- 1 On the main menu, tap **Phone Security**.
- 2 Enter your password.
- 3 Tap Security Options.
- 4 Tap Change Password.
- 5 In the Old Password field, enter the current password.
- 6 Enter the new password in both the New Password and Confirm Password fields.
The password must be numeric.
- 7 Unless you want to use password protection, select OK.

To set up password protection (password recovery)

- 1 Follow the preceding procedure to change your password, but do not select OK.
- 2 Select Use Password Protection.
- 3 In the Your Question and Your Answer fields, enter a question and answer that you can remember. Each field can accept up to 15 characters.
- 4 Select OK.

To recover a lost password

- 1 On the main menu, tap **Phone Security**.
If password protection is enabled, the Get button is available.

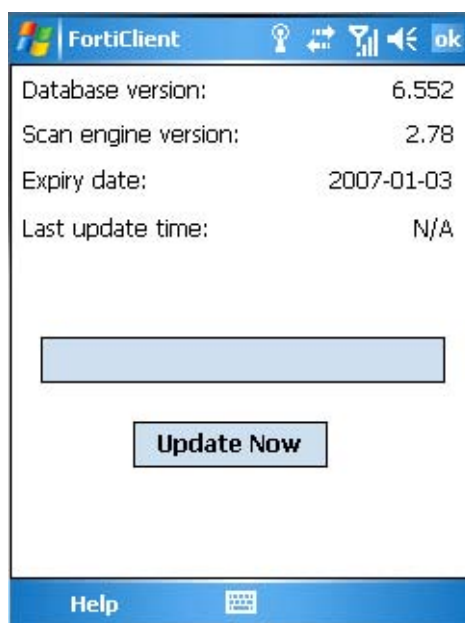
- 2 Tap Get.
- 3 Enter the preset question and answer in the Your Question and Your Answer fields and then select OK.
You must enter the question and answer exactly as you did when you set up password protection.
- 4 A message box displays your password.
- 5 Select OK.

Update

Your device needs to get AV signature and AV engine updates to guard against new viruses. You can view the current AV signature and AV scan engine version information on the Update page. From this page, you can also initiate an immediate update.

You can also configure your device to get updates from the server whenever a wireless connection is established or at a particular time every day. See [“System Options” on page 25](#).

Figure 13: Update page



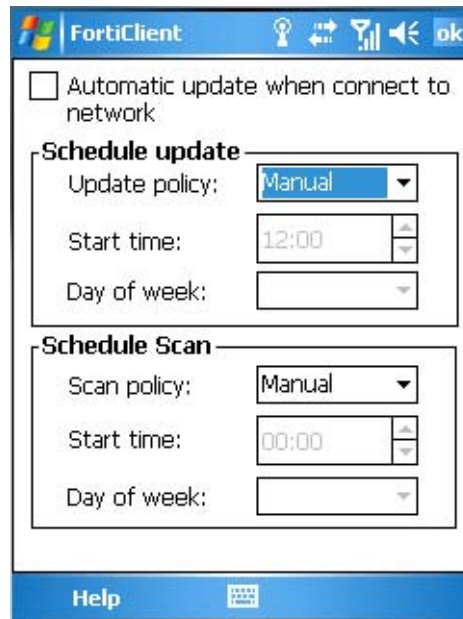
To initiate an immediate update

- 1 On the FortiClient main menu, tap the Update icon.
- 2 Tap Update Now. The update status bar displays the update progress.

System Options

You can set schedules for virus signature updates and antivirus scans.

Figure 14: System options



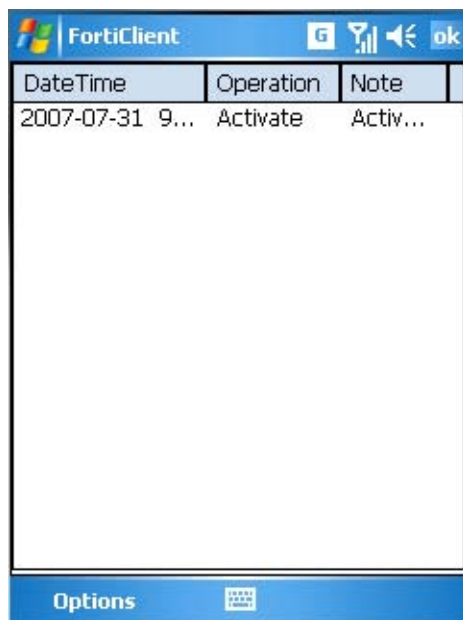
To configure automatic updates or antivirus scans

- 1 On the FortiClient Dashboard, tap **Control Center > System Option**.
- 2 To update virus signatures automatically when you connect to the network, select **Automatic update when connected to network**.
- 3 For **Schedule update** or **Schedule scan**, configure when they are performed:
 - **Manual** - there is no scheduled time, use Dashboard to initiate manually
 - **Daily**: select **Daily** policy and set the **Start time**
 - **Weekly**: select **Weekly** policy, set **Start time** and **Day of week**
 - **Monthly**: select **Monthly** policy, set **Start time** and **Day of month**
- 4 Tap **OK**.

Logs

The FortiClient program logs system events, virus detections, antispam actions and AV database updates. You can view or delete the logs. The headings in the log list depend on the type of log.

Figure 15: Logs



To view and manage logs

- 1 From the FortiClient main menu, tap the icon for the feature, followed by the icon for log access. For example, **Antivirus > Antivirus Log**.
- 2 Tap the log entry to read the details of a log.
- 3 Use the Options menu to manage logs:

Show details	Display detailed information about the selected log entry.
Delete	Delete the log entry.
Clear all	Delete all of the log entries on this page.

- 4 Tap OK.

Index

A

- ActiveSync 5
- answering machine 14
- antispam 17
 - blacklist 17
 - SMS 17
 - whitelist 17
- antivirus 11
 - scanning 11
 - setting scan schedule 25
 - start manual scan 12
- automatic update 25
- AV signature update
 - automatic 25
 - manual 24

B

- blacklist
 - antispam 17
 - Call Filter, editing 15

C

- call filter
 - black/white list 15
 - settings 15
- connecting
 - to a VPN 18
- contacts
 - encrypting 22

E

- encryption 19
 - of contacts 22
 - of files 20
 - of notes 21
 - options 22
 - setting password 22

F

- files
 - encrypting 20
- FortiTray menu 7
- forwarding
 - editing destinations 15

G

- greetings
 - selecting 15

H

- hardware platforms
 - supported 5

I

- incoming call filter 14
 - black/white list 15
 - settings 15
- installation 5

L

- logs
 - managing 26
 - viewing 26

M

- manual AV scan
 - antivirus 12
- manual update 24

N

- notepad
 - encryption 21

P

- password
 - for encryption 22

Q

- quarantine
 - view list of quarantined files 13

S

- scan
 - AV 11
- schedule
 - for updates and scans 25
- SMS antispam
 - enabling 17
- SMS text
 - editing messages 15
- system options 25

U

- update
 - AV engine and signature 24
 - setting schedule 25

V

VPN configuration 18

W

whitelist
 antispam 17
 Call Filter, editing 15
Windows Mobile versions
 supported 5



www.fortinet.com

FORTINET™

www.fortinet.com