

FortiClient Host Security for Windows Mobile Version 3.0

FORTINET™

www.fortinet.com

FortiClient Host Security for Windows Mobile User Guide
Version 3.0
January 15, 2007
04-30000-0247-20070115

© 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
Dashboard	8
Update.....	10
To initiate an immediate update.....	10
Antivirus scan	10
To enable real-time AV protection	11
To launch a manual AV scan.....	11
Quarantine files	12
VPN	13
To configure a VPN tunnel.....	13
To modify a VPN tunnel.....	13
To delete a VPN tunnel.....	13
To connect to a VPN.....	14
To disconnect from a VPN.....	14
To manually update VPN tunnel status	14
Firewall	14
To select the firewall protection level.....	14
SMS Antispam.....	15
To enable SMS antispam	15
To manage the WhiteList/BlackList	15
Address book protection	16
To enable address book protection	16
Schedule.....	17
To configure automatic updates or antivirus scans	17
Incoming call filter	18
Call Filter status	18
Call Filter settings.....	19
Working with lists	20
To add an entry to the list	20
To edit an entry in the list.....	20
To add an entry from your contact list	20
To delete an entry from the list	20

Logs..... **21**
 To view and manage logs..... 21

Index..... **23**

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](#)
- [Dashboard](#)
- [Antivirus scan](#)
- [VPN](#)
- [Firewall](#)
- [SMS Antispam](#)
- [Address book protection](#)
- [Schedule](#)
- [Incoming call filter](#)
- [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 [“Dashboard” 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 scan” on page 10](#).

Disable or Enable **SMSFilter**

Select to enable or disable the SMS Antispam filter. For more information, see [“SMS Antispam” on page 15](#).

Disable or Enable **CallWall**

Select to enable or disable incoming call management. For more information, see [“Incoming call filter” on page 18](#).

Switch Firewall to High Switch Firewall to Normal Switch Firewall to Low

Select to change the level of firewall protection. For more information, see [“Firewall” on page 14](#).

Hide FortiTray

Select to remove the FortiTray icon from the Today screen. To restore the FortiTray icon, tap **Start > Programs > FortiClient** to open the FortiClient Console, tap **Tools > Exit**, then restart the FortiClient application from the Start menu.

Dashboard

When you open the FortiClient console, FortiClient displays current operating information. To open the dashboard, select Open FortiClient Console from the FortTray menu or tap **Start > Programs > FortiClient**.

Figure 1: FortiClient dashboard



Shortcuts

Scan Device	Scan all or part of the device file system. See "To launch a manual AV scan" on page 11 . To configure scan settings, see "Antivirus scan" on page 10 .
Last scan	The date of the last file scan.
Update	Update virus signatures.
Last Update	The date of the last virus signature update.
Register	Enter your license key in the Serial number box and tap Register. You need to purchase the license key from Fortinet.
Expiry Date	The expiry date of your FortiClient application license.

FortiClient Status

	For each FortiClient feature, the current setting appears on the right. Tap to change it.
Realtime Monitor	Enable or disable real-time file protection. For more information, see "Antivirus scan" on page 10 .
Firewall	Set Firewall protection to Low, Normal or High. For more information, see "Firewall" on page 14 .
SMS Filter	Enable or disable SMS antispam filtering. For more information, see "SMS Antispam" on page 15 .
Incoming Call Filter	Enable or disable Incoming Call Filter. For more information, see "Incoming call filter" on page 18 .
Contacts Protection	Enable or disable Address Book protection. For more information, see "Address book protection" on page 16 .

Tools menu

Scan Device	Scan the file system of your device for viruses. See “To launch a manual AV scan” on page 11.
VPN	Use a Virtual Private Network (VPN) tunnel. For more information, see “VPN” on page 13.
Update	View the current antivirus database and scan engine version, expiry date and last update time. Select Update Now to download the latest virus signatures from FortiGuard. For more information, see “Update” on page 10.
Quarantine	View the list of quarantined files. Restore or delete quarantined files. See “Quarantine files” on page 12.
Call Filter	View status and configure Incoming Call Filter. See “Incoming call filter” on page 18.
Logs	View and clear logs. See “Logs” on page 21.
Exit	Exit FortiClient Console.

Options menu

Antivirus	Go to Antivirus settings. See “Antivirus scan” on page 10.
Firewall	Go to Firewall settings. See “Firewall” on page 14.
AntiSpam	Go to AntiSpam settings. See “SMS Antispam” on page 15.
Address Book	Go to Address Book protection settings. See “Address book protection” on page 16.
Schedule	Set schedule for virus signature updates and file scans. See “Schedule” on page 17.
Call Filter	Go to Incoming Call Filter settings. See “Incoming call filter” on page 18.

Help menu

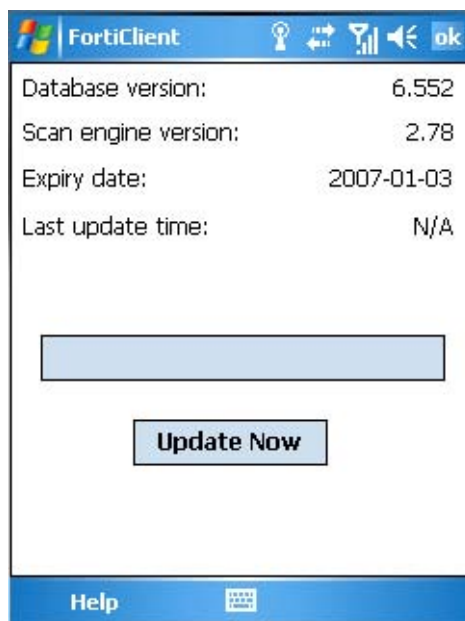
Help	Open the online Help.
Register	Enter your license key in the code box and tap Register. You need to purchase a license key from Fortinet.
About	View information about the FortiClient application.

Update

Your device needs to get AV signature and AV engine updates to guard against new viruses. You can configure your device to get updates from the server whenever a wireless connection is established or at a particular time every day. You can also initiate an update any time you like.

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

Figure 2: Update page



To initiate an immediate update

- 1 On the FortiClient Dashboard, tap Update or tap **Tools > Update**.
- 2 Tap Update Now. The update status bar displays the update progress.

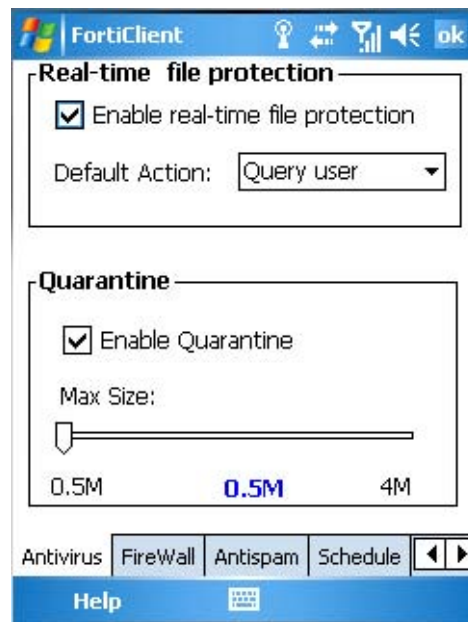
Antivirus scan

The FortiClient program protects your mobile device from virus attacks. It supports both on-demand (manual) and real-time file scanning.

Use on-demand scanning to specify file directories to scan for virus infections. Use real-time scanning to scan 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 [“Quarantine files” on page 12](#).

Figure 3: Antivirus tab



To enable real-time AV protection

- 1 On the FortiClient Dashboard, tap **Options > Antivirus**.
- 2 Tap Enable real-time file protection.
- 3 For Default Action, select one of the following options:
 - 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
- 4 Optionally, select Enable Quarantine and move the slider to select the amount of device memory to reserve for quarantined files. Deleted files are quarantined. When the 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 [“Quarantine files” on page 12](#).

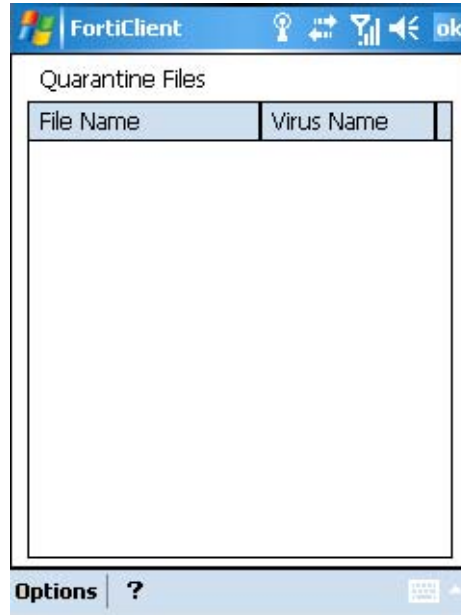
To launch a manual AV scan

- 1 On the FortiClient Dashboard, tap Scan Device or **Tools > Scan Device**.
- 2 Optionally, tap the ellipsis (...) button and select the path to scan. By default, the FortiClient application scans the entire device file system.
- 3 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.
- 4 After the scan is done, tap OK.

Quarantine files

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

Figure 4: Quarantine Files list



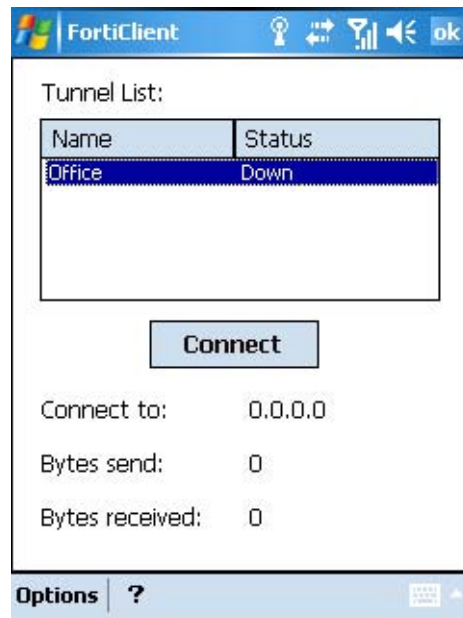
The Quarantine Files list shows the name of the virus detected in each quarantined file. Use the Options menu to see more information, restore or delete quarantined files.

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.

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 5: VPN tab



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 modify a VPN tunnel

You can modify only VPN tunnels that use automatic configuration.

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

To delete a VPN tunnel

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

To connect to a VPN

- 1 On the FortiClient Dashboard, tap **Tools > 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 Dashboard, tap **Tools > VPN**.
- 2 Tap the Disconnect button.

To manually update VPN tunnel status

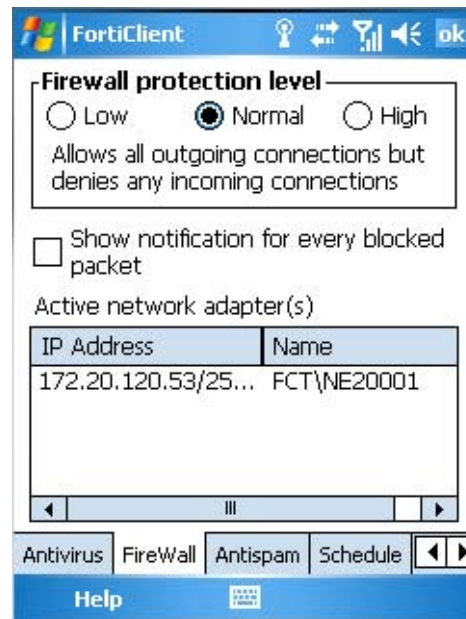
- 1 On the FortiClient Dashboard, tap **Tools > VPN**.
- 2 Tap **Options > Refresh**.

Firewall

Using the FortiClient firewall feature, you can protect your mobile device by selecting the proper firewall mode.

You can also view information about your mobile device's network adapter.

Figure 6: Firewall tab

**To select the firewall protection level**

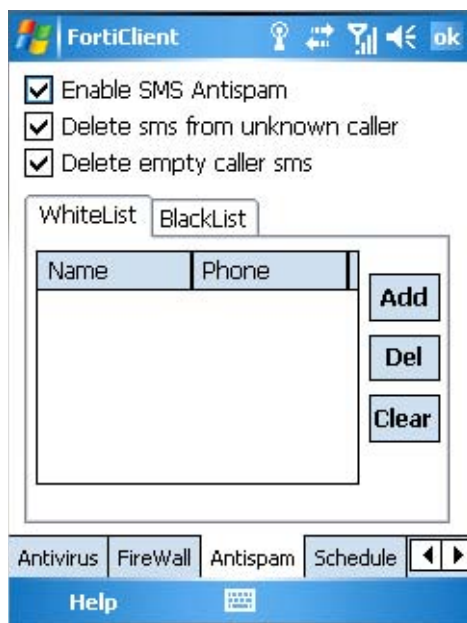
- 1 On the FortiClient Dashboard, tap **Options > Firewall**.
- 2 In the Firewall protection level section, select one of the following:
 - Low: Allows all traffic
 - Normal: Allows all outgoing connections but denies any incoming connections.
 - High: Blocks all incoming and outgoing traffic

- 3 If you want to be notified when packets are blocked, select Show notification for every blocked packet.
- 4 Tap OK.

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.

Figure 7: Antispam tab



To enable SMS antispam

- 1 On the FortiClient Dashboard, tap **Options > Antispam**.
- 2 To detect and block spam SMS messages, select Enable SMS Antispam.
- 3 To block specific numbers, add them to the Black list.
- 4 To block messages from callers that are not in your contact list, select Delete sms from unknown caller. If you want to allow specific callers not in your contact list, add them to the White list.
- 5 To block messages from unidentified callers, select Delete empty caller sms.
- 6 Tap OK.

To manage the WhiteList/BlackList

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

Address book protection

The FortiClient program protects your address book from being abused by malicious applications. If the address book feature is enabled, whenever an application attempts to access your address book, you will be prompted to allow or deny the access request. The application name is added to the Safe process list with access or deny status. This feature is available only on devices running Windows CE 2003.



Note: Pocket Outlook and programs in ROM are automatically granted permission. Only programs installed later require permission.

Figure 8: Address book protection tab



Enable address book protection Allow or deny access to the Address Book based on the Safe process list. If the application is not listed, the FortiClient application asks you whether to allow or deny access.

Switch Change status of selected application.

Delete Remove selected application from the Safe process list.

Empty Clear the Safe process list.

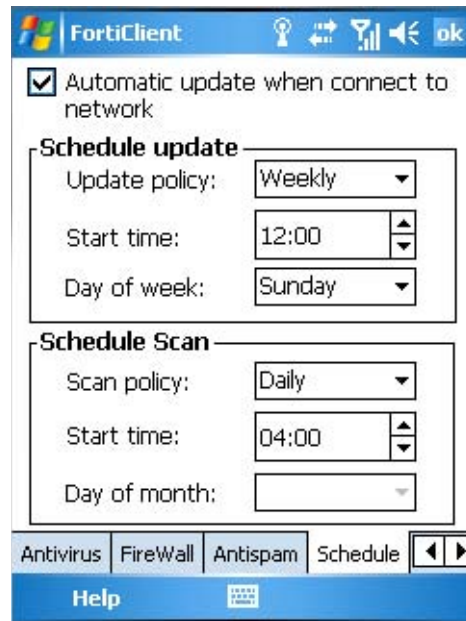
To enable address book protection

- 1 On the FortiClient Dashboard, tap **Options > Address Book**.
- 2 Select the Enable address book protection option.

Schedule

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

Figure 9: Schedule tab



To configure automatic updates or antivirus scans

- 1 On the FortiClient Dashboard, tap **Options > Schedule**.
- 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.

Incoming call filter

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

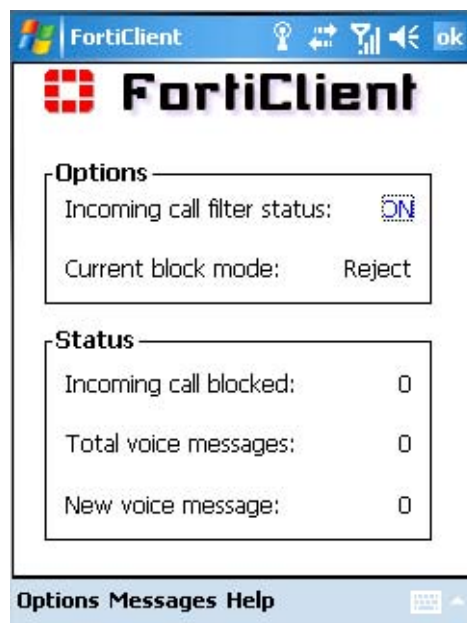
- block calls except for whitelisted callers, or callers in the Phonebook
- forward blocked callers to another number
- send blocked calls a text message
- enable blocked callers to leave a voice message

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

Call Filter status

Tap **Tools > Call Filter** to view the status of your incoming call filter.

Figure 10: Incoming call filter status



Options

- Incoming call filter status** Enable or disable the incoming call firewall.
- Current block mode** Call blocking mode currently selected. See [“Call Filter settings” on page 19](#).

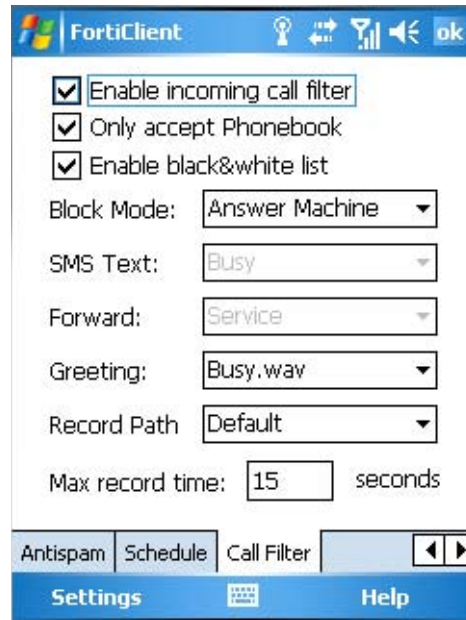
Status

- Incoming call blocked** The number of incoming calls that were blocked.
- Total voice messages** The number of voice messages received.
- New voice message** The number of voice messages you have not heard.

Call Filter settings

Tap **Options > Call Filter** to configure the incoming call filter.

Figure 11: 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 Answer Machine - enable caller to leave a voice message
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.
Greeting	Select a greeting for blocked callers when Block mode is Answer Machine. Select Settings > Greeting to create greetings. A greeting must be an audio file in WAV format.
Record Path	Select whether greeting files are in memory (default) or on a storage card.
Max record time	Select the maximum length for callers' voice messages.
Settings menu	Edit the Blacklist, Whitelist, SMS Text, Forwarding destinations or Greeting lists. See "Working with lists" on page 20 .

To configure blacklist, tap **Settings > Blacklist**.

To configure whitelist, tap **Settings > Whitelist**.

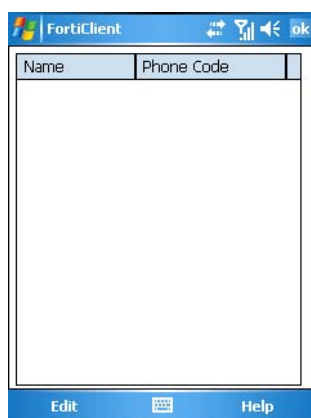
Working with lists

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
Greeting	Voice messages in WAV files that can be played to blocked callers when the Block mode is Answer Machine.

Tap **Options > CallFilter** and then tap the list name on the Settings menu.

Figure 12: 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.

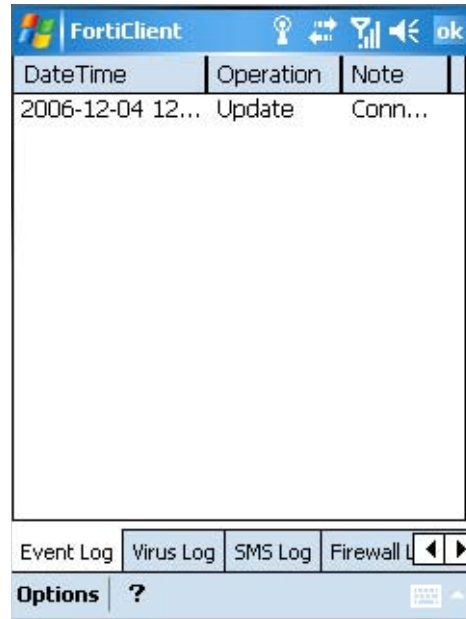
To delete an entry from the list

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

Logs

The FortiClient program logs all the events, such as virus detections and AV database updates. You can view or delete the logs.

Figure 13: Logs



To view and manage logs

- 1 On the FortiClient Dashboard, tap **Tools > Logs**.
- 2 Tap the tab for the type of log: Event, Virus, SMS, Firewall or Call Filter.
- 3 Tap the log entry to read the details of a log.
- 4 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.
- 5 Tap OK.

Index

A

- ActiveSync 5
- address book protection 16
 - enabling 16
- answering machine 18
- antispam 15
 - blacklist 15
 - SMS 15
 - whitelist 15
- antivirus 10
 - scanning 10
 - setting scan schedule 17
 - start manual scan 11
- automatic update 17
- AV signature update
 - automatic 17
 - manual 10

B

- blacklist
 - antispam 15
 - Call Filter, editing 20

C

- call filter settings 19
- connecting
 - to a VPN 14

D

- dashboard 8

F

- firewall
 - selecting the mode of 14
- firewall settings 14
- FortiTray menu 7
- forwarding
 - editing destinations 20

G

- greetings
 - selecting 20

H

- hardware platforms
 - supported 5
- Help menu
 - dashboard 9

I

- incoming call filter 18
 - settings 19
- installation 5

L

- logs
 - managing 21
 - viewing 21

M

- manual AV scan
 - antivirus 11
- manual update 10

O

- Options menu 9

Q

- quarantine
 - view list of quarantined files 12
- quarantine settings 11

R

- real-time AV protection 11
- register FortiClient 8

S

- scan
 - AV 10
 - manually, from Dashboard 8
- scan device
 - manually 9
- schedule
 - for updates and scans 17
- shortcuts
 - on dashboard 8
- SMS antispam
 - enabling 15
- SMS text
 - editing messages 20
- status
 - on dashboard 8

T

- Tools menu 9

U

update

- AV engine and signature 10
- from Dashboard 8
- setting schedule 17

V

VPN configuration 13

W

whitelist

- antispam 15
- Call Filter, editing 20
- Windows Mobile versions supported 5

FORTINET™

www.fortinet.com

FORTINET™

www.fortinet.com