



FortiClient Host Security
Version 3.0 MR4
Consumer Edition

FORTINET™

www.fortinet.com

FortiClient Host Security User Guide
Version 3.0 MR4
2 February 2007
04-30004-0271-20070202

© 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, FortiGate Unified Threat Management System, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, 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	5
FortiClient status icons.....	5
Using the FortiClient system tray icon menus	6
Documentation.....	6
Fortinet documentation CD	7
Fortinet Knowledge Center	7
Comments on Fortinet technical documentation.....	7
Customer service and technical support	7
Installation	9
System requirements	9
Language support	9
Installing FortiClient.....	10
Install log.....	10
General Settings.....	11
Entering a license key	11
Configuring proxy server settings	12
Antivirus.....	13
Scanning for viruses	13
Configuring antivirus settings.....	15
Selecting file types to scan or exclude	17
Selecting files and folders to exclude from scanning	17
Specifying an SMTP server for virus submission.....	18
Integrating FortiClient antivirus scanning with Windows shell.....	18
Configuring real-time protection	19
Configuring email scanning	20
Managing quarantined files	20
Monitoring Windows startup list entries	21
Restoring changed or rejected startup list entries	22
Firewall.....	23
Selecting a firewall mode.....	23
Selecting a firewall profile	23
Viewing traffic information	24
Configuring application access permissions	25
Managing address, protocol and time groups	26

Configuring network security zones	27
Adding IP addresses to zones	27
Customizing security settings	28
Configuring intrusion detection.....	29
Configuring advanced firewall rules.....	29
Managing groups	30
Web Filter.....	31
Setting the administration password	31
Configuring the web filter settings	32
Specifying URLs to block or bypass	33
AntiSpam	35
Installing antispam plug-in.....	36
Enabling antispam.....	36
Adding white, black, and banned word lists.....	36
Manually labelling email	37
Submitting misclassified email to Fortinet	38
Maintenance	39
Updating FortiClient.....	39
Backing up and restoring FortiClient settings	40
Logs	41
Configuring log settings	41
Managing log files	42
Saving FortiClient log information remotely	43
Index	45

Introduction

This chapter introduces you to FortiClient Host Security software and the following topics:

- [About FortiClient Host Security](#)
- [FortiClient status icons](#)
- [Using the FortiClient system tray icon menus](#)
- [Documentation](#)
- [Customer service and technical support](#)

About FortiClient Host Security

The FortiClient Host Security software is a secure remote access client for Windows computers. It integrates antivirus, antispam, Windows registry monitoring, firewall, and web browsing control into a single software package.

With the FortiClient software, you can:

- scan your computer for viruses,
- configure real-time protection against viruses and unauthorized modification of the Windows registry,
- restrict access to your system and applications by setting up firewall policies.
- restrict Internet access according the rules you specify.
- filter incoming email on your Microsoft Outlook® and Microsoft Outlook® Express to collect spam automatically.
- use the remote management function provided by the FortiManager System.

FortiClient status icons

The FortiClient status bar on the lower right corner displays the FortiClient status icons.



The antivirus scanning service is running.



The antivirus scanning service is stopped.



The update service is running.





The update service is stopped.



The real-time protection service is running.



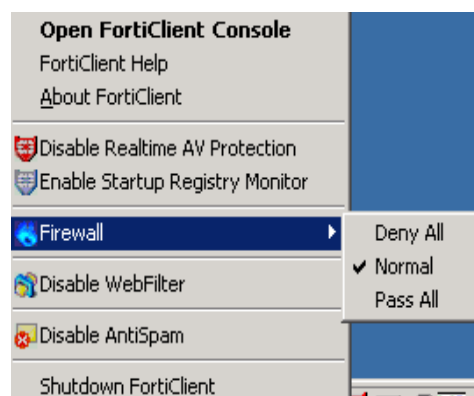
The real-time protection service is stopped.

-  Firewall protection is enabled.
-  Firewall protection is disabled.

Using the FortiClient system tray icon menus

Many of the frequently used FortiClient features are available from the system tray icon menus.

Figure 1: FortiClient system tray icon menus



Open FortiClient Console	Opens the management console so that you can configure the settings and use the services.
FortiClient Help	Opens the online help.
Enable/Disable Realtime AV Protection	For details, see “Configuring real-time protection” on page 19.
Enable/Disable Startup Registry Monitor	For details, see “Monitoring Windows startup list entries” on page 21.
Firewall	You can select Deny All, Normal, or Pass All. See “Selecting a firewall mode” on page 23.
Enable/Disable WebFilter	For details, see “Web Filter” on page 31.
Enable/Disable AntiSpam Filter	For details, see “AntiSpam” on page 35.
Shutdown FortiClient	Stops all FortiClient services and closes FortiClient console.

Documentation

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

Information about FortiGate Antivirus Firewalls is available from the FortiGate online help and the *FortiGate Administration Guide*.

Fortinet documentation CD

All Fortinet documentation is available from the Fortinet documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation see the Fortinet Knowledge Center.

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

For antivirus and attack definition updates, firmware updates, updated product documentation, technical support information, and other resources, please visit the Fortinet technical support web site at <http://support.fortinet.com>.

Fortinet email support is available from the following addresses:

amer_support@fortinet.com	For customers in the United States, Canada, Mexico, Latin America and South America.
apac_support@fortinet.com	For customers in Japan, Korea, China, Hong Kong, Singapore, Malaysia, all other Asian countries, and Australia.
eu_support@fortinet.com	For customers in the United Kingdom, Scandinavia, Mainland Europe, Africa, and the Middle East.

For information on Fortinet telephone support, see <http://support.fortinet.com>.

When requesting technical support, please provide the following information:

- Your name
- Company name
- Location
- Email address
- Telephone number
- FortiClient version
- Detailed description of the problem

Installation

The section describes:

- [System requirements](#)
- [Language support](#)
- [Installing FortiClient](#)
- [Install log](#)

The Windows executable file provides easy installation on a single computer. For details see [“Installing FortiClient” on page 10](#).

System requirements

To install FortiClient 3.0 you need:

- A PC-compatible computer with Pentium processor or equivalent
- Compatible operating systems and minimum RAM:
 - Microsoft Windows 2000: 128 MB
 - Microsoft Windows XP: 256 MB
 - Microsoft Windows Server 2003: 512 MB
 - Microsoft Windows XP 64-bit: 256 MB
- 100 MB hard disk space
- Native Microsoft TCP/IP communications protocol
- Native Microsoft PPP dialer for dial-up connections
- an Ethernet connection



Note: The FortiClient software installs a virtual network adapter.

Language support

The FortiClient Host Security user interface and documentation is localized for:

- English
- Simplified Chinese
- Japanese
- Korean

The FortiClient installation software detects which code page the computer is using and installs the matching language version. For any languages other than the above are detected, the English version of the software is installed.

Installing FortiClient

If you have an older version of FortiClient software installed on your computer, the Windows executable version of the installer automatically upgrades your FortiClient installation to the new version, retaining your current configuration. FortiClient 3.0 can reuse configuration data from FortiClient versions 2.0, 1.6 or 1.2, but not from version 1.0.



Note: For FortiClient version 1.0 and 1.2 installations, it is recommended that you uninstall the software before installing version 3.0 to ensure a clean install.

You can also perform an upgrade installation of FortiClient software using the .zip version of the installer, which contains an MSI installer package.

To install the FortiClient software

- 1 Double-click the FortiClient install program file.
- 2 Follow the instructions on the screen, selecting Next to proceed through the installation options.

You can perform either a complete installation or a custom installation that enables you to omit features you do not require.

The installation requires a reboot of the computer. Once the computer has rebooted, you can configure the FortiClient software.

To configure the FortiClient software after the system reboot

If you are upgrading the FortiClient software, you do not need to perform the following procedure.

- 1 On the FortiClient Configuration Wizard, select Basic Setup if you are installing FortiClient on a standalone computer, or select Advanced Setup if you are installing FortiClient on a computer in a network.
- 2 For Basic Setup, configure the update settings. For more update information, see [“Maintenance” on page 39](#).
- 3 For Advanced Setup, do the following:
 - Add IP addresses to FortiClient’s public, trusted, blocked zones. For more information, see [“Configuring network security zones” on page 27](#).
 - If your computer uses a proxy server, enter the proxy server information. See [“Configuring proxy server settings” on page 12](#).
 - Configure the update settings. See [“Maintenance” on page 39](#).

Install log

During the installation, FortiClient logs all install activities to a log file automatically. Should any problems arise during the install, you can review the install log to see where and when the issue occurred.

The install log file, fcinstalllog.txt is located in the following directory:

- on Windows 2000 in the c:\winnt\ directory.
- on Windows XP, in the c:\windows\ directory.

General Settings

Use the General Settings page to:

- set the FortiClient software to load automatically during startup,
- enable or disable real-time antivirus protection,
- enable or disable the Windows system startup list monitoring,
- enter a product license key,
- unlock the FortiClient software if it is locked by FortiManager,
- configure the proxy server settings.

You can also use the General Settings page to view:

- the current version and serial number of the FortiClient software,
- the current version of the antivirus definition files,
- the time of the last antivirus scan,
- the status of the auto-update service.
- the time of the last update.

Entering a license key

The FortiClient software uses license keys to distinguish between evaluation software and fully licensed software.

Evaluation software provides fully functional firewall features. Antivirus updates are available for 90 days, antispam and web-filtering services are available for 90 days. You cannot extend the evaluation period by reinstalling the software.

When you purchase and enter a license key into the software, antivirus updates are available until the license expires. The General > Status page displays the license serial number and expiry date.

To use antispam and web filtering services beyond the evaluation period, you must purchase a FortiGuard service subscription. For more information, see <http://www.fortinet.com/products/fortiguard.html>.

Contact your local Fortinet sales engineer or <https://shop.fortinet.com> or visit <http://www.fortinet.com/products/forticlient.html> to buy or renew a license key.

To enter a license key

- 1 Go to **General > Status**.
- 2 Select Enter License Key.
- 3 Enter the license key.
- 4 Select OK.

Configuring proxy server settings

If you use a proxy server for your LAN, you can specify the proxy server settings so that the FortiClient software can go through the proxy server to get antivirus signature updates and submit viruses.

FortiClient software supports HTTP, SOCKS v4, and SOCKS v5 proxy protocols.

To configure proxy server settings

- 1 Go to **General > Connection**.
- 2 Select **Enable proxy for updates and/or Virus Submission**.
- 3 For **Proxy Type**, select **HTTP**, **SOCK V4**, or **SOCK V5**.
- 4 Enter the proxy server's IP address and port number.
- 5 Enter the user name and password.
- 6 Select **Apply**.



Note: You can get the proxy server information from your network administrator.

Antivirus

Using the FortiClient antivirus feature, you can protect your computer by regularly scanning the computer for viruses. The FortiClient software can also perform real-time virus protection and monitor Windows Registry changes.

Scanning for viruses

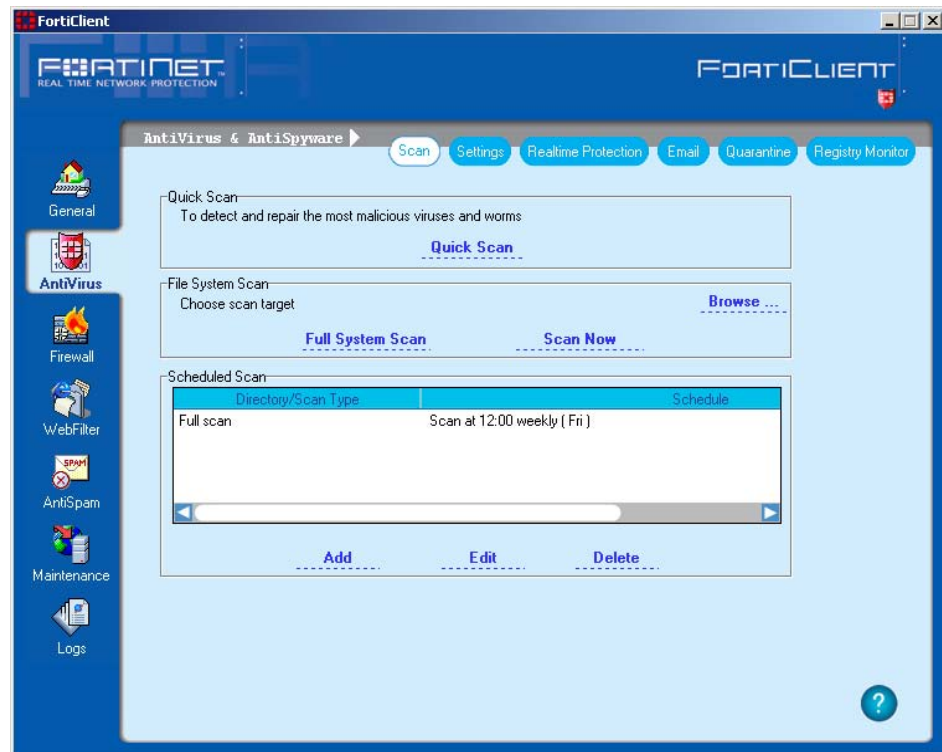
You can run a quick scan to detect the most malicious viruses and worms. You can also set up scan schedules and scan the files in a specified folder.

Depending on the option you choose on the Antivirus Settings tab, the FortiClient software does one of the following when it finds any viruses:

- Displays a virus alert message.
- Quarantines the virus-infected file.
- Cleans the virus-infected file.

For information about how to configure what happens when the FortiClient software finds a virus, see [“Configuring antivirus settings” on page 15](#).

Figure 2: Scanning for viruses



To run a quick scan

- 1 Go to **Antivirus > Scan**.
- 2 Select Quick Scan.
The Antivirus Scanning dialog box opens, displaying the scanning process and results. The infected file list displays the names of any infected files.
- 3 Optionally, select Stop to stop the scanning process before it completes.
- 4 Optionally, right-click on entries in the Infected file list and choose one of the following actions: Delete, Quarantine, Submit Virus to Fortinet, Submit as false positive to Fortinet.
- 5 To view the detailed summary of the scanning process after the scan is finished, select View Result.

To scan files in a specified directory

- 1 Under File System Scan, select Browse to locate the directory to scan.
- 2 Select Scan Now.
The Antivirus Scanning dialog box opens, displaying the scanning process and results. The infected file list displays the names of any infected files.
- 3 Optionally, right-click on entries in the Infected file list and choose one of the following actions: Delete, Quarantine, Submit Virus to Fortinet, Submit as false positive to Fortinet.

To perform a full system scan

- 1 Under File System Scan, select Full System Scan.
- 2 Select Network drives and/or Removable media if you want them included in the scan. Optionally, you can change the relative priority of virus scanning compared to other processes.
- 3 Select Start.
The Antivirus Scanning dialog box opens, displaying the scanning process and results. The infected file list displays the names of any infected files.
- 4 Optionally, right-click on entries in the Infected file list and choose one of the following actions: Delete, Quarantine, Submit Virus to Fortinet, Submit as false positive to Fortinet.

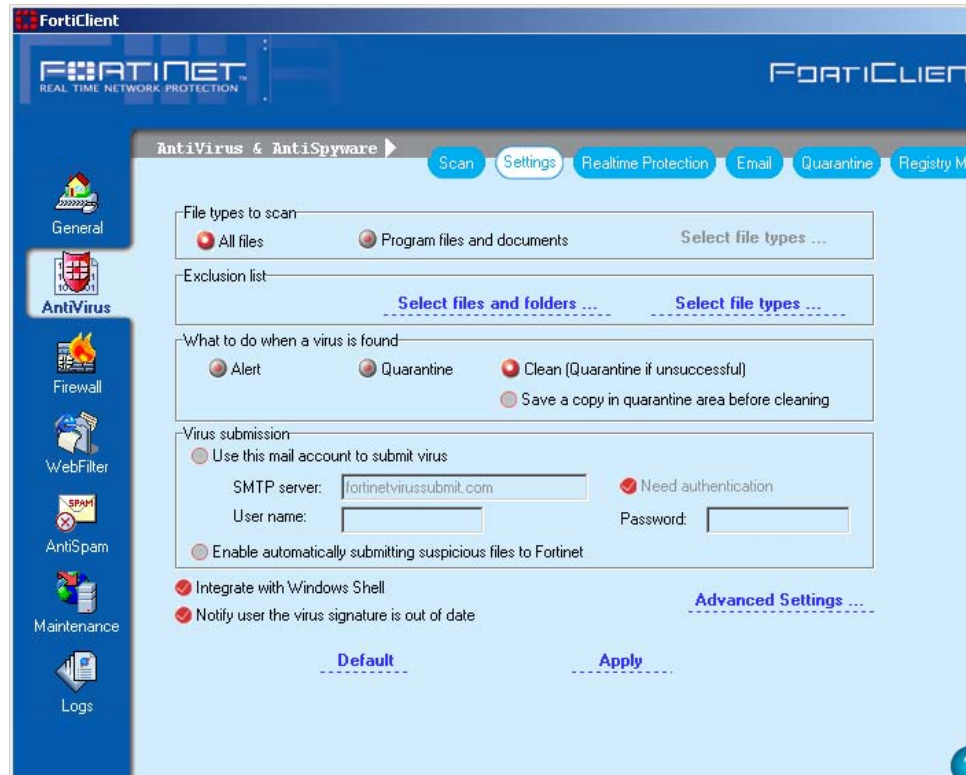
To manage scan schedules

- 1 To add a schedule, select Add.
- 2 In the New Schedule dialog box, set up a new schedule.
You can set up daily, weekly, or one-time schedules. You can also specify which folder to scan.
- 3 To modify a schedule, select the schedule and then select Edit.
- 4 To delete a schedule, select the schedule, then select Delete.

Configuring antivirus settings

You can specify what types of files to scan and what to do when a virus is detected. You can also specify an SMTP server to use when submitting a quarantined file to Fortinet for analysis. For information on how to submit a quarantined file, see [“Managing quarantined files” on page 20](#).

Figure 3: Configuring antivirus settings



The default antivirus settings are listed in [Table 1](#).

Table 1: Default antivirus settings

Configuration Option	Setting
File types to scan	All files
What to do when a virus is found	Clean
Enable automatically submitting suspicious files to Fortinet	Enabled
Integrate with Windows Shell	Enabled
Notify user the virus signature is out of date	Enabled

To configure the antivirus settings

- 1 Go to **Antivirus > Settings**.
- 2 Select the file types to be scanned.
- 3 Add or delete file types to be scanned for viruses. See [“Selecting file types to scan or exclude” on page 17](#).

- 4 Select files, folders and file types to be excluded from virus scanning.
 - To exclude a file or folder, click the Select file and folders button, then select Add to add the file or folder to the exemption list.
 - To exclude a file type, click the Select file types button, then add the file types. For more information, see [“Selecting file types to scan or exclude” on page 17](#).
- 5 Select what to do when a virus is found. The default is Clean.
 - Alert - display a message is displayed if a virus is detected during real-time file system monitoring.
 - Quarantine - move the file to a quarantine directory
 - Clean - attempt to remove the virus from the infected file. If this is not possible, move the file to the quarantine area. If you want to save a copy of the virus, select Save a copy in quarantine area before cleaning.
- 6 Configure the settings to submit viruses. See [“Specifying an SMTP server for virus submission” on page 18](#).
- 7 If you want to add a FortiClient antivirus scan command to the Windows Explorer shortcut menu, select Integrate with Windows shell. See [“Integrating FortiClient antivirus scanning with Windows shell” on page 18](#).
- 8 Optionally select the Notify user the virus signature is out of date option.
- 9 Optionally select Advanced Settings.

On the Advanced Settings dialog box, you can:

 - specify whether to scan the compressed files and the file size limit. The default size limit is 0, which means no limit.
 - specify whether to scan grayware and what types of grayware to look for.
 - enable heuristic scanning. FortiClient software uses heuristic techniques to scan files to find the unknown viruses and threats that have not yet been cataloged with signatures. Heuristics looks at characteristics of a file, such as size or architecture, as well as behaviors of its code to determine the likelihood of an infection.

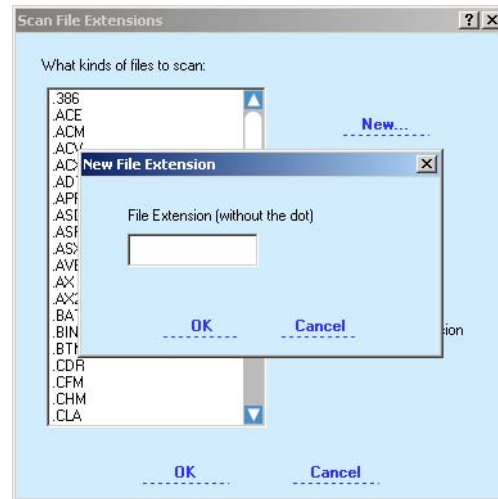
Selecting file types to scan or exclude

If you do not want the FortiClient software to scan all files for viruses, you can select file types from the default list of file types. You can add file types to or delete file types from the default file types list. You can create a list of file types to exclude from virus scanning. You can also reset the file types list to defaults.



Note: The exclusion list takes priority over the inclusion list. For example, if you select a file extension to scan, and also add the same file extension to the exclusion list, the files with this extension will not be scanned.

Figure 4: Adding a new file extension



To add a new file type to the file types or exclusion list

- 1 Go to **Antivirus > Settings**.
- 2 Under File types to scan, select Program files and documents.
- 3 Under either File types to scan or Exclusion list, click Select file types.
- 4 Select New.
- 5 Type the file extension to add to the list. You can add file types with double extensions.
- 6 Select OK.



Note: Scanning files with no extension is enabled by default.

Selecting files and folders to exclude from scanning

There may be some folders or specific files that you do not want FortiClient software to scan for viruses. You can add these files and folders to the files and folders exclusion list.

To add files and folders to the exclusion list

- 1 Go to **Antivirus > Settings**.
 - 2 Click Select files and folders.
- The AntiVirus Options window opens.

- 3 Select Add
- 4 Navigate to the desired file or folder and select it.,
- 5 Select OK.
- 6 Add or remove other files and folders as needed.
- 7 Select OK.

To remove files and folders from the exclusion list

- 1 Go to **Antivirus > Settings**.
- 2 Click Select files and folders.
The AntiVirus Options window opens.
- 3 Select the file or folder that you want to remove from the list.
- 4 Select Delete.
- 5 Add or remove other files and folders as needed.
- 6 Select OK.

Specifying an SMTP server for virus submission

Instead of using the default mail server, you can specify an SMTP server to use when submitting the quarantined files.

To specify an SMTP server

- 1 Go to **Antivirus > Settings**.
- 2 Under Virus Submission, select Use this mail account to submit virus.
- 3 For SMTP server, enter the SMTP server that you use for outgoing email.
- 4 If the SMTP server needs authentication to log on, select Need authentication and enter the logon user name and password.
- 5 Select Apply.

Integrating FortiClient antivirus scanning with Windows shell

By integrating FortiClient antivirus scanning with Windows shell, you can use the FortiClient antivirus shortcut menu in Windows Explorer to scan the selected folders or files for viruses.

To integrate with Windows shell

- 1 Go to **Antivirus > Settings**.
- 2 Select Integrate with Windows Shell.
- 3 Select Apply.

In Windows Explorer, you can right-click on folders or files and select Scan with FortiClient Antivirus to scan them.

Configuring real-time protection

Configure the real-time protection settings to specify what types of files to scan and exclude and what happens when a virus is detected during real-time system monitoring.

To configure real-time protection

- 1 Go to **Antivirus > Realtime Protection**.
- 2 In File types to scan, select either All files or Program files and documents, as needed.
If you select Program files and documents, you can modify the list of file types to be scanned. See [“Selecting file types to scan or exclude” on page 17](#).
- 3 Optionally, select files, folders and file types to be excluded from virus scanning.
 - To exclude a file type, see [“Selecting file types to scan or exclude” on page 17](#).
 - To exclude a file or folder, see [“Selecting files and folders to exclude from scanning” on page 17](#).
- 4 Under What to do when a virus is found, select Deny Access, Quarantine or Clean.

Deny Access	You cannot open, run or modify the file until it is cleaned.
Quarantine	The file is moved to a quarantine directory.
Clean	The FortiClient agent attempts to remove the virus from the infected file. Clean is selected by default. Optionally, select Save a copy in quarantine area before cleaning.



Note: If FortiClient cannot clean an infected file, it quarantines the file automatically.

- 5 Select or clear the following two options:
 - Do not pop up alert message box in real-time scan.
 - Do not pop up alert message box in registry monitor.
- 6 Optionally select Advanced Settings.
On the Advanced Settings dialog box, you can:
 - specify whether to scan the compressed files and the file size limit. The default size limit is 0, which means no limit.
 - specify whether to scan grayware and what types of grayware to look for.
 - enable heuristic scanning. FortiClient software uses heuristic techniques to scan files to find the unknown viruses and threats that have not yet been cataloged with signatures. Heuristics looks at characteristics of a file, such as size or architecture, as well as behaviors of its code to determine the likelihood of an infection. You can choose to deny access to files heuristics finds suspicious or to only display a warning.
 - enable scanning of files when written to or read from disk, optionally including files on network drives.
- 7 Select Apply.

Configuring email scanning

FortiClient software can scan incoming and outgoing email and email attachments for viruses and worms.

FortiClient software can also use heuristic techniques to scan email attachments to find unknown viruses and threats that have not yet been cataloged with signatures. Heuristics looks at the characteristics of a file, such as size or architecture, as well as the behavior of its code to determine the likelihood of an infection.

To scan email for viruses

- 1 Go to **Antivirus > Email**.
- 2 In the Virus scanning section, select SMTP for outgoing mail, POP3 for incoming mail and MS Outlook if Outlook connects to a Microsoft Exchange server.
- 3 To prevent worms from spreading via email, select Enable email worm detection. Then select what to do when a malicious action is detected: either immediately terminate the offending process or ask the user whether to terminate the process. This is available only if you selected SMTP Virus scanning.
- 4 To apply heuristic scanning, in the Heuristics scanning section, select Enable email attachments heuristics scanning. Then select what to do when a suspicious attachment is detected: either Log a warning message or Strip and quarantine.

Managing quarantined files

Quarantined files remain in the quarantine directory until you delete them or restore them to their original location.

Through the default mail server or the SMTP server you specify, you can submit the quarantined file to Fortinet for analysis. For information on how to specify an SMTP server, see [“Specifying an SMTP server for virus submission” on page 18](#).



Caution: Quarantined files may still be infected. Check the status of a quarantined file before restoring.

To manage quarantined files

- 1 Go to **Antivirus > Quarantine**.
- 2 From the quarantined file list, select the file(s).
 - to restore the file to its original location, select Restore.
 - to delete the file, select Delete.
 - to send the file to Fortinet, select Submit > Submit virus.
 - to alert Fortinet if you believe that the quarantined file is not a virus, select Submit > Submit as false positive.



Note: You can submit a maximum of three quarantined files a day.

- 3 Optionally select Refresh to refresh the quarantined file list.

Monitoring Windows startup list entries

Some viruses can modify existing Windows registry entries or insert new entries to cause malicious code to be executed when you start or log on to Windows. The FortiClient software can monitor the Windows startup list and detect unauthorized changes to the registry. The FortiClient software assumes the following registry changes are unauthorized if the changes were not made by an authorized user:

- adding, removing or modifying an application installation,
- changing an existing application's configuration settings.



Note: Monitoring the Windows Registry is not supported on 64-bit Microsoft Windows XP.

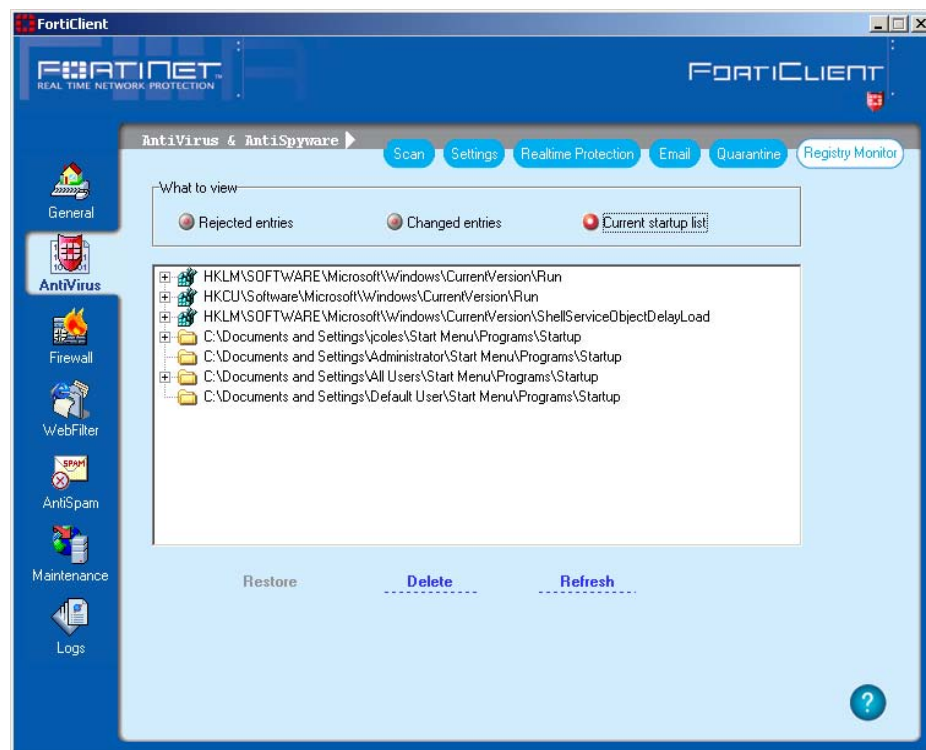
The startup list shows the Windows registry entries for any applications that are started as part of your Windows profile when you log on to Windows. The list includes applications that are displayed in the system tray. The list also includes any applications that are started transparently and are not displayed in the system tray.

Entries are displayed in three lists:

- The Rejected entries list displays new, unauthorized startup entries.
- The Changed entries list displays previously existing entries that have changed since the last Windows startup.
- The Current startup list displays all current registry entries.

The startup list is checked when the FortiClient software starts.

Figure 5: Registry Monitor



To view Windows startup list entries

- 1 Go to **Antivirus > Registry Monitor**.
- 2 Under What to view, select Rejected entries, Changed entries or Current startup list.
- 3 Optionally select Refresh to refresh the startup list entries to view recently added, changed or rejected registry entries.

Restoring changed or rejected startup list entries

Changed or rejected entries can be restored.



Caution: If you are unsure what application an entry is for, do not restore the startup list entry.

To restore a changed or rejected startup list entry

- 1 Go to **Antivirus > Registry Monitor**.
- 2 Under What to view, select Changed entries or Rejected entries.
- 3 Select the entry you want to restore.
- 4 Select restore.

Firewall

Using the FortiClient firewall feature, you can protect your computer by using the following FortiClient firewall features:

- **Application level network access control.**
You can specify the applications that can access the network and be accessed by the network.
- **Network security zone.**
The network is categorized into three zones: Public Zone, Trusted Zone, and Blocked Zone.
- **Intrusion detection.**
FortiClient firewall can detect and block the common network attacks.
- **Advanced firewall rules.**
You can create specific rules to control the traffic based on source addresses, destination addresses, protocols, or time frames.

For outbound traffic, only application level control rules are applied. The advanced firewall rules do not have effect.

For inbound traffic, the advanced firewall rules will be applied first, then the application control rules.

For the traffic related to system process, such as NetBIOS, the traffic is only accepted when it is allowed by both advanced rules and zone security settings.

Selecting a firewall mode

By default, FortiClient firewall runs in Normal mode to protect your system. You can go to **Firewall > Status** to select a different firewall mode (protection level).

FortiClient firewall has the following running modes:

Deny all	Blocks all the incoming and outgoing traffic.
Normal	You can select from the three protection profiles. See "Selecting a firewall profile" on page 23 .
Pass all	No firewall protection.

Selecting a firewall profile

If you select the Normal firewall mode on **Firewall > Status**, you can select from the following firewall protection profiles:

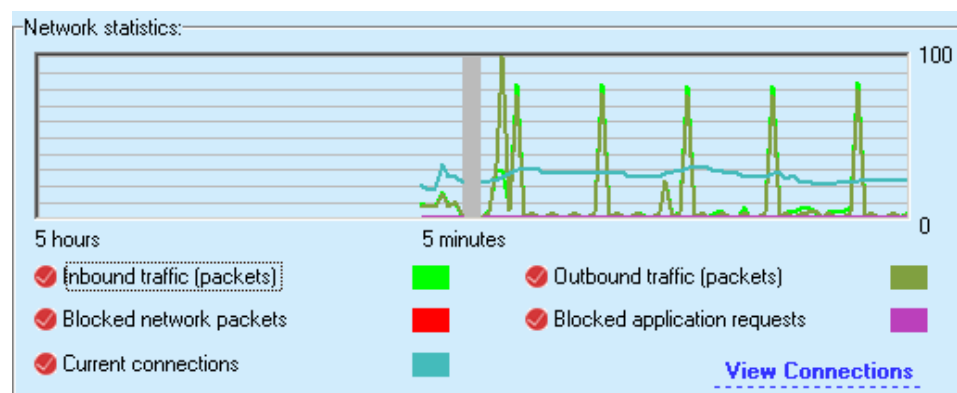
Basic home use	Allows all outgoing traffic and denies all incoming traffic. Select this profile if your PC is a standalone home computer and not connected to other networks or PCs.
-----------------------	---

Basic business	Allows all outgoing traffic, allows all incoming traffic from the trusted zone, and denies all incoming traffic from the public zone. For zone information, see “Configuring network security zones” on page 27.
Custom profile	This is the default profile. The Custom profile allows you to configure the application level permissions, network zone permissions, and advanced firewall filtering rules. See “Configuring application access permissions” on page 25, “Configuring network security zones” on page 27, and “Configuring advanced firewall rules” on page 29.

Viewing traffic information

You can configure the FortiClient software to display the following network traffic information:

Figure 6: Firewall status



Inbound traffic	Number of incoming network packets.
Outbound traffic	Number of outgoing network packets.
Blocked network packets	Network packets that are blocked by the firewall.
Blocked application request	Number of blocked requests from outside to access your local applications and vice versa.
Current connections	Number of current connections between your system and the network.

To view the traffic information

- 1 Go to **Firewall > Status**.
- 2 Select the traffic type you want to view. The information displays in the graphical monitor.
- 3 Select **View Connections** to view the current active connections, listening ports, PID, and other detailed information.
- 4 Select **Close**.

- 5 By default, whenever FortiClient firewall blocks network traffic, a notification pops up at the FortiClient system tray icon area. To disable the blocked traffic notification, select the Disable taskbar notification for blocked network traffic option.

Configuring application access permissions

You can specify the applications that can access the network and be accessed by the network. To do this, you assign the applications access permissions. Three levels of access permissions are available:

Allow	Allows application access request without asking.
Ask	Prompts to ask your permission for the incoming or outgoing access requests.
Block	Blocks all access requests.



Note: Applications not listed in the access control list will be asked for network access attempts. By default, FortiClient allows the legitimate Windows system applications to access the network. These applications are displayed in the application control list. You can modify or delete the permission levels of these applications.



Note: You cannot edit or delete settings for the fortiproxy application.

Apart from application access control, network zone security, and intrusion detection, FortiClient firewall protects your computer with another layer of security: advanced firewall rules.

The firewall rules allow or block network traffic according to the following three types of filtering criteria you specify:

- **Source and destination addresses** can be your own computer, one of the two zones (Public Zone and Trusted Zone), a single IP address, a range of IP addresses, a subnet, or a address group. For information about adding an address group, see [“Managing groups” on page 30](#).
- **Network protocols** can be TCP, UDP, or TCP/UDP.
- **Day and Time** ranges can be applied to a rule to restrict access based on the day of the week and the time of day.

The advance firewall rules take precedence over the zone security settings. For example, if a rule blocks the traffic to the Trusted Zone, the traffic will be blocked.

To add an application to the access control list

- 1 Go to **Firewall > Applications**.
- 2 Select Add.
- 3 In the Add New Application dialog box, enter or browse to the application path.
- 4 Select permission levels for the public zone and trusted zone.
- 5 Select OK.



Note: Permission levels for the public zone can only be lower than or equal to those for the trusted zone.

To create a firewall rule

- 1 Go to **Firewall > Applications**.
- 2 Select **Edit > Advanced > Add**.
- 3 In the Advanced Firewall Filtering Rule dialog box, enter the following information and select OK.

Name	Enter a name for the rule.
Description	Optionally, enter a short description.
State	Either Enable or Disable the rule.
Action	Either Allow or Block the traffic.
Source	Apply the rule to the traffic that originates from the source address and terminates at your computer. Select Add to add the source address. For information about adding an address group, see "Managing address, protocol and time groups" on page 26 .
Destination	Apply the rule to the traffic that originates from my computer and terminates at the destination address. Select Add to add the destination address. For information about adding an address group, see "Managing address, protocol and time groups" on page 26 .
Protocol	Select Add to add a protocol to the rule. While specifying the protocol in the Add Protocol dialog box, you can also specify the destination and source ports.
Time	Select add to add a day/time range when the rule should be executed. In the Add Time dialog box, specify a description, time range and one or more days. Time range is specified using a 24 hour clock.
Bind this rule to	Select all adapters or a single ethernet adapter on your computer to apply this rule.



Note: You can use any combination of the filtering criteria.

Managing address, protocol and time groups

To simplify management, you can combine the source addresses, destination address, protocols, and time schedules into groups and use the groups when creating rules.

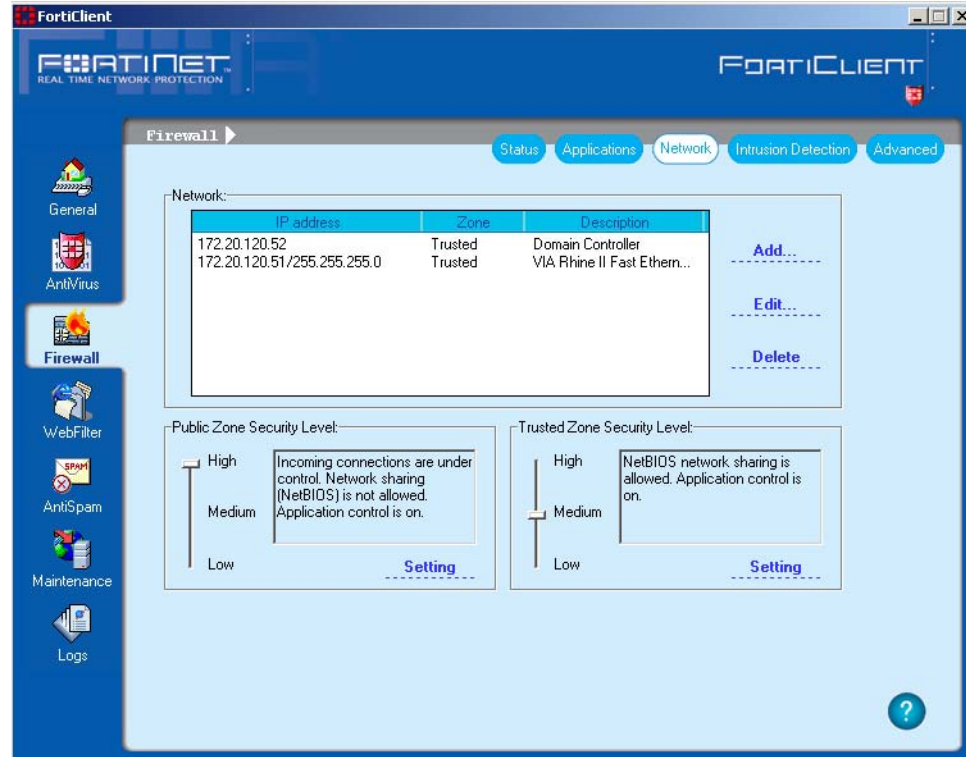
To create a group

- 1 Go to **Firewall > Applications**.
- 2 Select **Edit > Advanced > Groups**.
- 3 Select **Address Group, Protocol Group, or Time Group**.
- 4 Select **Add**.
- 5 Enter a name and description.
- 6 Select **Add**.
- 7 For an address group, enter the subnet, IP range, or IP address. For a protocol group, enter specify the protocol and port number. For a time group, specify the day and time range.
- 8 Select **OK**.

Configuring network security zones

FortiClient firewall protects your system by categorizing the network systems into three zones.

Figure 7: Network security zones



Public Zone

By default, FortiClient firewall treats IP addresses in the public zone with the highest security level. You can also customize the security levels. See [“Customizing security settings” on page 28](#).

Trusted Zone

By default, FortiClient firewall treats IP addresses in the trusted zone with medium-level security settings. For information about security level settings, see [“Customizing security settings” on page 28](#).

Blocked Zone

All traffic to and from IP addresses in the blocked zone is not allowed.

FortiClient firewall prioritizes the zones in the order of blocked zone, trusted zone, and public zone. This means:

- If an IP address is listed in all of the three zones, it will be blocked.
- If it is listed in both the trusted and public zones, it will be trusted.
- If it is not listed in any of the three zones, it will be public.

Adding IP addresses to zones

You can add a subnet, an IP range, or an individual IP address to the network zones. You can also edit or delete the existing IP entries.

To add IP addresses

- 1 Go to **Firewall > Network**.
- 2 Select **Add**.

- 3 In the IP Address dialog box, select a zone and enter the IP addresses.
- 4 Optionally, enter a description.
- 5 Select OK.

Customizing security settings

For the public and trusted zones, you can use the default high, medium, or low level security settings. You can also customize these default settings.

High	By default, incoming connections are allowed only if there are listening ports for these connections.
Medium	By default, most connections are allowed unless you customize the settings. Note that the default medium security level settings for public and trusted zones are different: <ul style="list-style-type: none"> • For public zone, the incoming ICMP and NetBIOS packets are blocked • For trusted zone, these packets are allowed.
Low	Packet level rule is disabled and application level control is on.



Note: The security level for the public zone can only be higher than or equal to that for the trusted zone.

To customize the security settings

- 1 Go to **Firewall > Network**.
- 2 For Public Zone Security Level or Trusted Zone Security Level, move the slider to High or Medium.



Note: Low level security disables packet level rules and you cannot customize the Low level settings.

- 3 Select Settings.
- 4 If you select High level, modify the following settings and select OK.

Allow ICMP in	Allows incoming ICMP (Internet Control Message Protocol) traffic. By default, this option is not selected.
Allow NetBIOS in	Allows incoming NetBIOS traffic. By default, this option is not selected.
Allow NetBIOS out	Allows outgoing NetBIOS traffic. By default, this option is not selected.
Allow other inbound traffic coming from this zone	This option is selected by default.
Block other inbound traffic coming from this zone	This option is not selected by default.

- 5 If you select Medium level, modify the following settings and select OK.

Block ICMP in	Blocks incoming ICMP (Internet Control Message Protocol) traffic. By default, this option is not selected.
Block NetBIOS in	Blocks incoming NetBIOS traffic. By default, this option is not selected.
Block NetBIOS out	Blocks outgoing NetBIOS traffic. By default, this option is not selected.

Configuring intrusion detection

FortiClient software can detect and block some common network attacks using the hard-coded signatures. Because the signatures are hardcoded into the program, to get the latest signatures, you must install the latest FortiClient build.

Go to **Firewall > Intrusion Detection** to view the IP addresses where the detected attacks originate.

You can move the IP addresses to the blocked zone by selecting the Move to blocked zone button, so that the traffic from these IP addresses will be blocked.

If any of the IP addresses can be trusted, you can move the IP address to the trusted IP list by selecting the Trust this IP button, so that FortiClient will not detect traffic from this IP address any more.

You can also remove an IP from the Trusted IP list by selecting the Don't trust this IP button.

Configuring advanced firewall rules

Apart from application access control, network zone security, and intrusion detection, FortiClient firewall protects your computer with another layer of security: advanced firewall rules.

The firewall rules allow or block network traffic according to the following three types of filtering criteria you specify:

- **Source and destination addresses** can be your own computer, one of the two zones (Public Zone and Trusted Zone), a single IP address, a range of IP addresses, a subnet, or a address group. For information about adding an address group, see ["Managing groups" on page 30](#).
- **Network protocols** can be TCP, UDP, or TCP/UDP.
- **Day and Time** ranges can be applied to a rule to restrict access based on the day of the week and the time of day.

The advance firewall rules take precedence over the zone security settings. For example, if a rule blocks the traffic to the Trusted Zone, the traffic will be blocked.

To create a firewall rule

- 1 Go to **Firewall > Advanced**.
- 2 Select Add.

- 3 In the Advanced Firewall Filtering Rule dialog box, enter the following information and select OK.

Name	Enter a name for the rule.
Description	Optionally, enter a short description.
State	Either Enable or Disable the rule.
Action	Either Allow or Block the traffic.
Source	Apply the rule to the traffic that originates from the source address and terminates at your computer. Select Add to add the source address. For information about adding an address group, see "Managing groups" on page 30 .
Destination	Apply the rule to the traffic that originates from my computer and terminates at the destination address. Select Add to add the destination address. For information about adding an address group, see "Managing groups" on page 30 .
Protocol	Select Add to add a protocol to the rule. While specifying the protocol in the Add Protocol dialog box, you can also specify the destination and source ports.
Time	Select add to add a day/time range when the rule should be executed. In the Add Time dialog box, specify a description, time range and one or more days. Time range is specified using a 24 hour clock.
Bind this rule to	Select all adapters or a single ethernet adapter on your computer to apply this rule.



Note: You can use any combination of the filtering criteria.

Managing groups

To simplify management, you can combine the source addresses, destination address, protocols, and time schedules into groups and use the groups when creating rules.

To create a group

- 1 Go to **Firewall > Advanced**.
- 2 Select Groups.
- 3 Select Address Group, Protocol Group, or Time Group.
- 4 Select Add.
- 5 Enter a name and description.
- 6 Select Add.
- 7 For an address group, enter the subnet, IP range, or IP address. For a protocol group, enter specify the protocol and port number. For a time group, specify the day and time range.
- 8 Select OK.

Web Filter

You can use the FortiClient web filtering feature to control web access according to the rules you specify. For instance, you can use the FortiClient predefined web access profile for children to prevent your children from accessing the unhealthy web sites.

FortiClient software uses the FortiGuard-web filtering service to help you control the web URL access.

FortiGuard-Web is a managed web filtering solution provided by Fortinet. FortiGuard-Web sorts hundreds of millions of web pages into a wide range of categories users can allow, block, or monitor. Your FortiClient PC accesses the nearest FortiGuard-Web Service Point server to determine the category of a requested web page. Then the FortiClient software decides either to allow or block the web page according to the categories you specify.

In addition to the control of web category access, FortiClient also allows you to specify URLs to block or bypass.

Setting the administration password

You must set a password to prevent users from modifying the web filter settings, shutting down the program, or uninstalling the program.

To set the password

- 1 Go to **WebFilter > WebFilter**.
- 2 Select Change Password.
- 3 Enter a password and select OK.

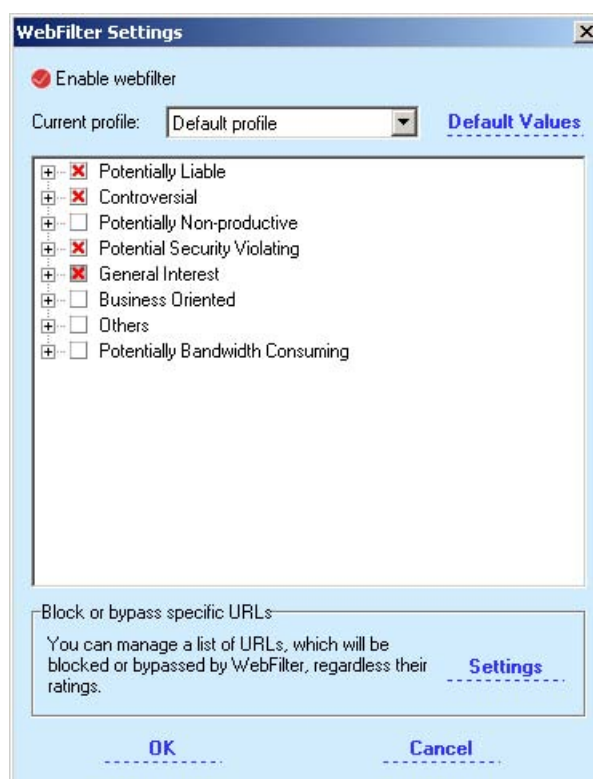
Configuring the web filter settings

FortiGuard-Web includes over 60 million individual ratings of web sites applying to hundreds of millions of pages. Pages are sorted and rated into 56 categories and these categories are divided into eight larger groups for easy management.

FortiClient comes with three predefined profiles to allow or block different combinations of the web categories.

Default	Default web filter settings, which are the same as those of the Child profile.
Child	Blocks the categories that are not suitable for children.
Adult	Only blocks the security violating web sites.

Figure 8: Web filter settings



To configure the web filter settings

- 1 Go to **WebFilter > WebFilter**.
- 2 Select Modify Settings.
- 3 Enter the password if you already set one.
- 4 In the Web Filter Settings dialog box, select Enable webfilter.
- 5 Select a profile from the Current profile list.
- 6 You can modify the category list if required. To cancel the modifications and use the default settings instead, select Default Values.
- 7 Select OK.

Specifying URLs to block or bypass

You can specify the exact URLs to block. You can also specify the URLs to bypass the block category.

To specify URLs to block or bypass

- 1 Go to **WebFilter > WebFilter**.
- 2 Select Modify Settings.
- 3 In the WebFilter Settings dialog box, select Settings.
- 4 In the Block or bypass specific url dialog box, select Add.
- 5 In the Set url permission dialog box, enter the URL.
In the URL box, you can enter:
 - wildcard characters (* and ?) in URLs,
 - complete URLs,
 - IP addresses,
 - partial URLs,
 - file types, such as *.jpg to block all jpeg files, and *.swf to block all flash animations.
- 6 Select Block or Bypass.
- 7 Select OK.

AntiSpam

The antispam feature is a plug-in for Microsoft Outlook and Microsoft Outlook Express (2000 or newer versions). It is supported by the Fortinet FortiGuard AntiSpam service. Once this feature is enabled and installed on the Outlook/Outlook Express, it filters your incoming email and sets up a spam folder on your Outlook/Outlook Express to collect spam automatically.



Note: AntiSpam is not available on Microsoft Windows Vista.

You can do the following:

- [Installing antispam plug-in](#)
- [Enabling antispam](#)
- [Adding white, black, and banned word lists](#)
- [Manually labelling email](#)
- [Submitting misclassified email to Fortinet](#)

Figure 9: AntiSpam

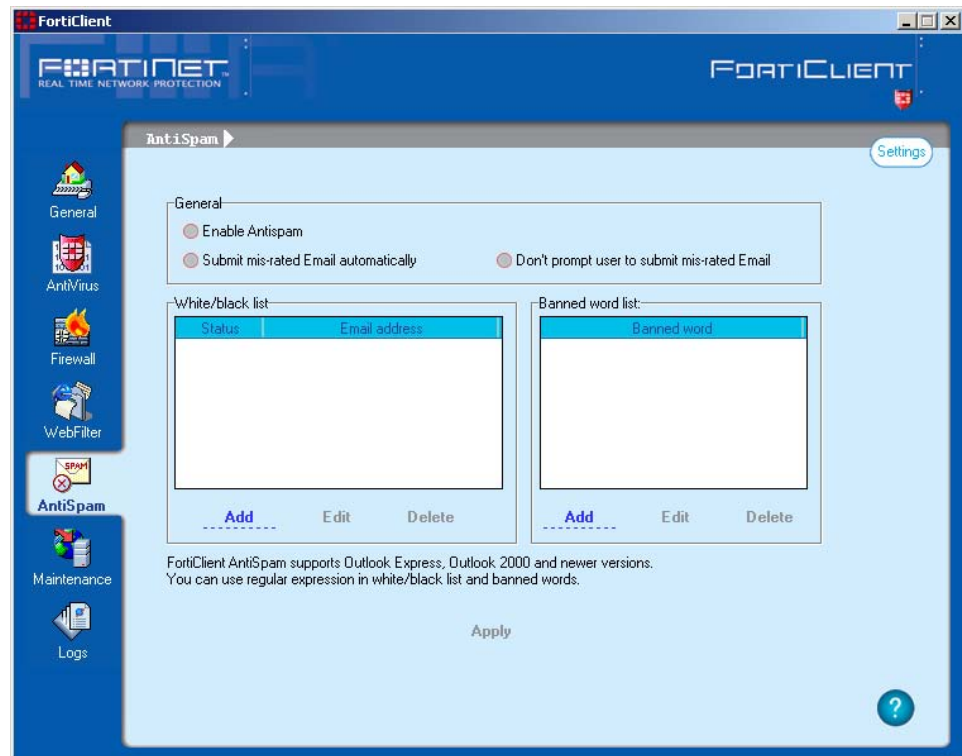
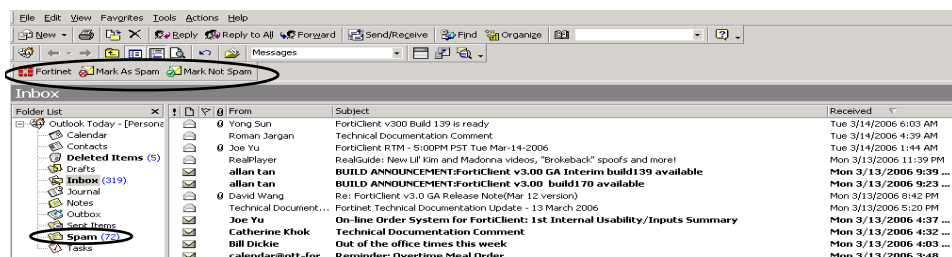


Figure 10: Antispam plug-in on Outlook



Installing antispam plug-in

Install the antispam plug-in on Microsoft Outlook or Outlook Express (2000 or newer version).

To install antispam plug-in on Outlook

- 1 On your PC, install Microsoft Outlook or Outlook Express if you do not already have it.
- 2 Install FortiClient software.
- 3 Reboot your PC.

A Spam folder appears on the Outlook folder List. Spam sent to you will be put into the Spam folder automatically.

Fortinet website, Mark As Spam and Mark Not Spam icons appear on the Outlook toolbar.

Enabling antispam

You must enable the FortiClient antispam feature for the Outlook plug-in to work.

To enable antispam

- 1 Go to **AntiSpam > Settings**.
- 2 Select **Enable AntiSpam**.
- 3 Select **Apply**.

Adding white, black, and banned word lists

You can allow (whitelist) or block (blacklist) email addresses and ban email containing the words you specify. By doing so, incoming email will be first filtered against these lists.

- If the email address is in the white list and the email content does not contain any of the banned words, the email will go through without being filtered.
- If the email address is in the black list or the email content contains any of the banned words, the email will be sent to the spam folder.

- If the email address is neither in the white list or black list and the email content does not contain any of the banned words, the email will be filtered by the Fortinet FortiGuard AntiSpam service.



Note: When adding banned words and email addresses to the White/black list, you can use regular expression meta characters.

To add white/black lists

- 1 Go to **AntiSpam > Settings**.
- 2 In the White/black list panel, select Add.
- 3 Enter the email address that you want to block or allow.
- 4 Select Block to add the address to black list, and Allow to add it to white list.
- 5 Select OK.
- 6 To modify a list item, select the item, then Edit.
- 7 To remove a list item, select the item, then Delete.

To add banned words

- 1 Go to **AntiSpam > Settings**.
- 2 In the Banned word list panel, select Add.
- 3 Enter the word that you want to ban.
- 4 Select OK.
- 5 To modify a list item, select the item, then Edit.
- 6 To remove a list item, select the item, then Delete.

Manually labelling email

You can manually mark an email as a spam or as an innocent mail.

If you have not enabled the FortiClient Submit mis-rated Email automatically function, you will be prompted to submit a selected email to Fortinet when you mark an email as a spam or as an innocent mail. Otherwise, the selected email will be sent to Fortinet automatically to train its FortiGuard database. For more information, see [“Submitting misclassified email to Fortinet” on page 38](#).

To manually mark an email as spam

- 1 Open Microsoft Outlook or Outlook Express.
- 2 If you find a spam in your Inbox folder, select the email.
- 3 Select the Mark As Spam icon on the toolbar.

The email is sent to the Spam folder. If it is also forwarded to Fortinet, when you update the FortiClient software next time, the Outlook plug-in will update its spam database so that when an email from the same sender/address comes in again, it will be sent to the Spam folder.

To manually mark an email as an innocent mail

- 1 Open Microsoft Outlook or Outlook Express.
- 2 If you find an innocent email in your Spam folder, select the email.
- 3 Select the Mark Not Spam icon on the toolbar.

The email is sent to the Inbox folder. If it is also forwarded to Fortinet, when you update the FortiClient software next time, the Outlook plug-in will update its spam database so that when an email from the same sender/address comes in again, it will not be sent to the Spam folder.

Submitting misclassified email to Fortinet

You can configure the FortiClient program to automatically send misclassified email, that is, innocent email classified as spam or spam classified as innocent email, to the Fortinet FortiGuard AntiSpam service to enhance the service's email-scanning accuracy. In this case, you will not be prompted to submit misclassified email manually.

You can also just configure the FortiClient program to stop prompting users to submit misclassified email manually. In this case, no misclassified email will be sent to Fortinet.

For more information, see [“Manually labelling email” on page 37](#).

To configure sending misclassified email to Fortinet

- 1 Go to **AntiSpam > Settings**.
- 2 Select Submit mis-rated Email automatically.
- 3 Select Apply.

To stop prompting users to submit misclassified email manually

- 1 Go to **AntiSpam > Settings**.
- 2 Select Don't prompt users to submit mis-rated email.
- 3 Select Apply.

Maintenance

You can use the Update feature to update the AV definition and AV engine. With the Backup/Restore feature, you can save all the FortiClient settings to a file. If required, you can later load this file to restore all settings.

Updating FortiClient

You can view the current AV definition and AV engine version information and configure updates on the Update page.

Each copy of the FortiClient software has a unique identifier called UID. The UID is displayed at the upper right corner of the Update page. Whenever FortiClient sends out an update request, it also sends out the ID number. If you encounter any update problem, Fortinet technical support can use this number to pinpoint the problem.

If the FortiClient computer uses a proxy server, you can specify the proxy server settings so that the FortiClient software can get updates through the proxy server. See [“Configuring proxy server settings” on page 12](#).

Updates can be run manually or scheduled to run automatically on a daily basis.

To initiate immediate updates

- 1 Go to **Maintenance > Update**.
- 2 Select Update Now.

Under Update Status, you can view the update process and results.

To schedule updates

- 1 In the Update Schedule section, select Enable schedule update daily at and enter the time of day to perform the update.
- 2 Select Apply.



Note: The default update server is forticlient.fortinet.com. If you want to use a different server, select the Use this server to update option at the top of the update page and enter the URL of the update server. You do not need to specify http:// or https:// as part of the URL.

To manually update the software and antivirus signatures

- 1 Download the FortiClient update package file (.pkg file) to the FortiClient computer.
- 2 Go to **Maintenance > Update** and select Manual Update.
- 3 In the Open dialog box, locate the update package file and select Open.

Backing up and restoring FortiClient settings

If you have administrative privileges on your computer, you can save all FortiClient settings to a file so that you can easily restore them at a later date. For example, if you are forced to reinstall the software after replacing a hard drive, loading a backup will restore FortiClient to the same settings it had when you made the backup. You can also use a single backup file to configure multiple FortiClient installations with identical settings.

To back up the FortiClient settings

- 1 Go to **Maintenance > Backup/Restore**.
- 2 Select Backup.
- 3 Enter a file name and location in the Save As dialog box.
- 4 Enter a password in the Input Password dialog box. Enter the password again in the confirmation field to ensure you typed it correctly. Remember this password because you must enter it correctly when you restore the backup file.

To restore the FortiClient settings

- 1 Go to **Maintenance > Backup/Restore**.
- 2 Select Restore.
- 3 Choose the file you want to restore in the Open dialog box.
- 4 Enter the password associated with the file.

FortiClient will restore the configuration and close. Restart FortiClient to complete the procedure.

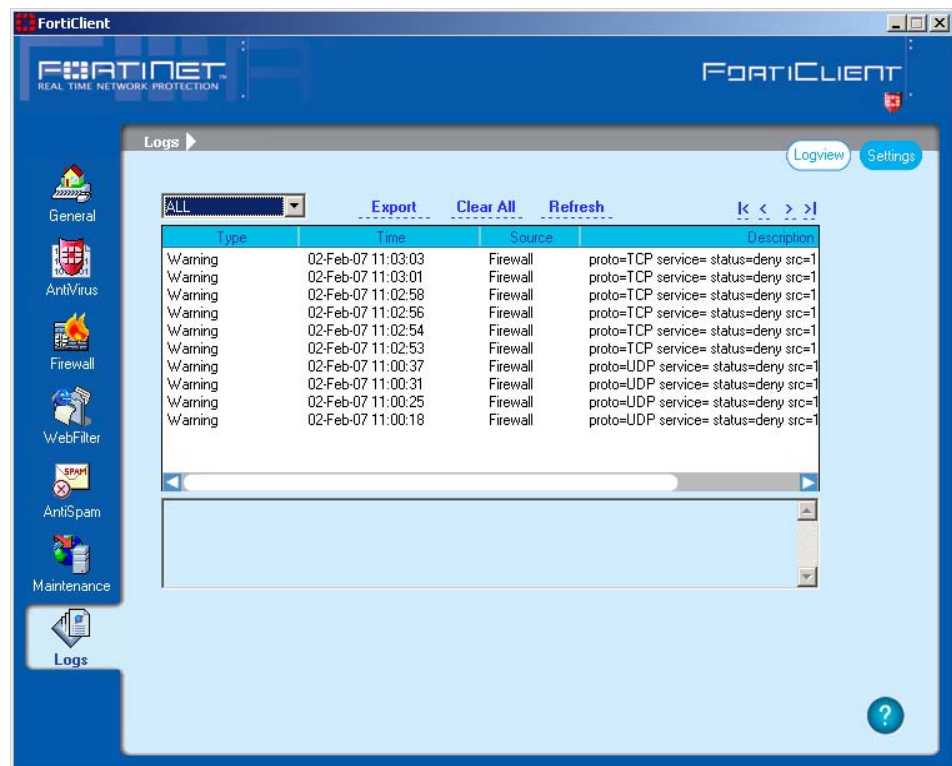
Logs

Use the FortiClient logging feature to configure logging of different types of events for any or all of the FortiClient services.

Configuring log settings

You can specify the log level, log type, log size, and log entry lifetime.

Figure 11: Configuring log file settings



To configure log settings

- 1 Go to **Logs > Settings**.
- 2 Enter the Maximum Log Size.

The default is 5120 KB. Log entries are overwritten, starting with the oldest, when the maximum log file size is reached.

3 Enter the Maximum Life Time.

The default is 0 days. A maximum life time of 0 days means log entries are kept until the maximum log size is reached. These log file entries are deleted once they reach the specified maximum life time.



Note: If the log file reaches either the specified maximum file size or the specified maximum life time, whichever comes first, the oldest log entries will be deleted.

4 Select the Log Level.

You can select Error, Warning or Information. The default is Warning.

5 Select what to log.

You can select either All events or Check to select. If you choose Check to select, specify the types of events to log.

6 Select Apply.

To configure remote logging

1 Go to **Logs > Settings**.

2 Select Server and enter the server IP address or FQDN in the adjacent box.

3 Select FortiLog if you are using a FortiLog or FortiAnalyzer unit to record logs, otherwise select Syslog.

4 From the Facilities list, select the name used to identify this FortiClient PC in the logs. The default is local7.

5 If you are logging to a syslog, from the Syslog log level list, select the minimum severity of logs to record.

6 Select Apply.

Managing log files

The log viewer can display logs of all events or only the events associated with a specific service. You can view, save, clear, or refresh the log entries.

To manage the log messages

1 Go to **Logs > Logview**.

2 From the dropdown list, select the log entry type you want to view.

3 Use the log navigation buttons to move between log entries or to move to the top or bottom of the log file. The most recent log entries are displayed at the top of the list.

Optionally select a specific log entry from the log window to view the complete log entry information.

4 To save the log messages, select Export.

5 To delete all the log messages, select Clear All.

6 To display the most recent log messages, select Refresh.

Saving FortiClient log information remotely

The FortiClient software can send logging information to a remote server in Syslog format. The server must have an application running capable of receiving Syslog formatted logs.

To send FortiClient logs to a Syslog server

- 1 Go to **Logs > Settings**.
- 2 Select **Server** and enter the Syslog server IP address in the adjacent field.
- 3 Change the **Facilities** setting if required. The Syslog facilities setting is one of the information fields associated with a Syslog message. If each FortiClient installation is configured to use a different facility setting, you can easily determine which FortiClient installation a log message came from.
- 4 Select **Syslog** to enable the sending of log information in Syslog format.
- 5 In **Syslog log level**, select the minimum log severity to send to Syslog.
- 6 Select **Apply**.

Index

A

- antispam
 - enabling 36
- antispam plug-in
 - installing 36
- antivirus 13
- antivirus settings
 - configuring 15

C

- code page 9
- comments on Fortinet technical documentation 7
- configuration
 - option 15
- configuration data 10
- customer service and technical support 7

E

- email
 - manually labelling 37
- email scanning 20
- entering a license key 11
- exclude
 - selecting the file types to exclude 17
- exclusion list
 - adding a new file extension 17

F

- file extension
 - add to the file types or exclusion list 17
- file types
 - adding a new file extension 17
 - selecting the file types to scan or exclude 17
- FortiClient software
 - manual update 39

G

- general settings 11

I

- icon
 - status 5
- install
 - configuration 10
 - data 10
 - log 10
 - upgrade 10
- installation 9
- introduction 5
- intrusion detection 29

K

- key
 - entering a license key 11

L

- language support 9
- license key
 - enter 11
 - entering 11
- log file
 - configuring settings 41
 - viewing 42
- logging 10
- logs 41
 - managing log files 42

M

- manage
 - log files 42
 - quarantined files 20
 - scan schedules 14
- mis-rated email
 - submitting 38

P

- protection
 - configuring real-time 19

Q

- quarantined files
 - managing 20
- quick scan
 - running 14

R

- real-time protection
 - configuring 19
- restore
 - changed startup list entry 22
 - quarantined file 20
 - rejected startup list entry 22

S

- scan
 - files in a specified directory for viruses 14
 - for viruses 13
 - selecting the file types to scan 17
- settings
 - general 11

startup list entries
 viewing 22
startup list entry
 restoring a changed or rejected startup list entry 22
status icons 5

U

update
 FortiClient software 39

update schedule
 setting 39
upgrading 10
URL
 block or bypass 33

W

web filter 31
 configuring 32

FORTINET™

www.fortinet.com

FORTINET™

www.fortinet.com