



User Guide

Optenet Security Suite PC

Version 10.09.39

COPYRIGHT

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Optenet S.A., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

Optenet, EDUNET, COTENET, E-Optenet, Optenet.BE, Optenet.CL, Optenet.CO.CR, Optenet.COM.EC, EDUNET.COM.ES, Optenet.COM.ES, EDUNET.ES, Optenet.ES, Optenet.US, Optenet.FR, OBTENET.COM, OBTENET.NET, Optenet.COM, Optenet.NET, CAPITANNET.COM, CAPITANNET.ORG, CAPITANNET.NET, CAPITANET.COM, CAPITANET.ORG, CAPITANET.NET, Optenet.BIZ, PROTEGELES.COM, PROTEGELES.NET, PROTEGELES.ORG, SURF-MATE.COM, SURF-MATE.NET, SURF-MATE.ORG, PROTEGELOS.COM, PROTEGEALOSNINOS.COM, SIFT-PLATFORM.ORG, Optenet.COM.GT, Optenet.COM.HN, Optenet.COM.MX, Optenet.COM.PA, Optenet.COM.PE, PTENET.CO.UK (in process), Optenet.COM.VE, are registered trademarks or trademarks of Optenet S.A. and/or its affiliates in Spain and/or other countries. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSE SOFTWARE.

TABLE OF CONTENTS

TABLE OF CONTENTS	4
1 INTRODUCTION.....	6
1.1 OPTENET SECURITY SUITE	6
1.2 MAIN FEATURES OF OPTENET SECURITY SUITE	6
1.3 OPTENET SECURITY SUITE WEB FILTER	7
1.4 OPTENET SECURITY SUITE ANTI-VIRUS.....	7
1.5 OPTENET SECURITY SUITE ANTI-SPAM.....	7
1.6 OPTENET SECURITY SUITE ANTI-PHISHING	7
1.7 OPTENET SECURITY SUITE FIREWALL	7
1.8 PROTOCOL FILTERING	8
1.9 EFFECTIVENESS.....	8
1.10 OPTENET SECURITY SUITE LANGUAGES	8
1.11 BROWSING SPEED WHEN USING OPTENET SECURITY SUITE	8
1.12 WEB FILTER SECURITY.....	9
1.13 UNBLOCKING SERVICE FOR PAGES BLOCKED IN ERROR	9
1.14 ACTIVATION OR DEACTIVATION OF THE SECURITY SUITE	9
1.15 BLOCKING P2P FILE SHARING AND DOWNLOADING OF PROGRAMS	9
1.16 BLOCKING INSTANT MESSAGING PROGRAMS	9
1.17 BLOCKING EMAIL.....	9
1.18 UPDATES	9
2 TECHNICAL REQUIREMENTS	10
2.1 TECHNICAL KNOWLEDGE	10
2.2 SYSTEM COMPATIBILITY	10
3 INSTALLATION PROCESS	11
4 CONFIGURATION.....	17
5 GENERAL.....	19
5.1 SERVICE STATUS	19
5.2 CHANGE PASSWORD	20
5.2.1 Changing the Administrative Password.....	21
5.2.2 Changing Password Recovery Question/Answer and Email Address	22
5.3 UPGRADING (SOFTWARE UPDATE)	24
5.4 ADVANCED OPTIONS	24
5.5 PROXY SETTINGS	24
6 WEB FILTER	26
6.1 CONFIGURATION	26
6.1.1 Filter Status: Activate/Deactivate	27
6.1.2 Internet blocked due to repeated attempts to access forbidden pages	27
6.1.3 Selecting Web Categories to block.....	27
6.1.4 SafeSearch	29
6.1.5 File types to be filtered	29
6.1.6 Browsing schedules.....	30
6.2 PERSONAL URL LISTS (BLACK & WHITE LISTS).....	31
6.3 REPORTS (BROWSING HISTORY)	31
6.4 FILTERING PROFILES	32
6.4.1 Enabling/Disabling the use of Profiles.....	33
6.4.2 Creating a new profile	34
6.4.3 Configuring/Editing a profile.....	34
6.4.4 Deleting a filtering profile.....	37

6.5	CONTRIBUTION – ADD WEBSITES TO THE FILTER	38
6.6	ADVANCED CONFIGURATION	39
6.7	PROTOCOL FILTERING	40
6.7.1	P2P	41
6.7.2	Instant Messaging	41
6.7.3	Email.....	41
6.7.4	Newsgroups.....	41
6.7.5	Chat.....	42
6.7.6	Virtual Worlds.....	42
6.7.7	Other	42
6.8	REINFORCING THE BLOCKING	43
7	ANTI-VIRUS	44
7.1	PROTECTION LEVEL	44
7.2	ANALYSIS	45
7.3	WATCHING AGENT.....	47
7.4	UPDATING.....	48
7.5	ANTI-VIRUS REPORTS.....	48
7.6	QUARANTINE	49
8	FIREWALL	51
8.1	SECURITY LEVEL.....	51
8.2	APPLICATION CONTROL.....	52
8.3	NETWORK ENTRIES.....	55
8.4	IP CONFIGURATION (IP BLACK & WHITE LISTS)	55
8.5	SERVICE CONFIGURATION	56
8.6	PROTOCOLS.....	58
8.7	REPORTS.....	58
9	ANTI-SPAM.....	60
9.1	OPTIONS.....	60
9.2	PERSONAL LISTS (BLACK & WHITE LISTS)	61
9.3	ADVANCED CONFIGURATION	61
9.4	QUARANTINE	62
9.4.1	Quarantine Configuration.....	64
9.5	REPORTS.....	64
10	ANTI-PHISHING.....	66
10.1	OPTIONS.....	66
10.2	PERSONAL LISTS (BLACK & WHITE LISTS)	67
10.3	PERSONAL DATA PROTECTION	68
10.4	QUARANTINE	70
10.4.1	Quarantine Configuration.....	72
10.5	REPORTS.....	72
11	REPORTS	74
12	CONTACT SUPPORT	75
13	UN-INSTALL	76



1 INTRODUCTION

1.1 Optenet Security Suite

Optenet Security Suite is a tool that optimizes Internet usage and provides the highest levels of security. It offers the most effective protection on the market for both IT equipment and Users.

This is achieved through the combination of highly effective individual components.

In addition, Optenet Security Suite is a transparent application that does not affect the functioning of other applications, system performance, or the speed of communications.

Optenet Security Suite is the most advanced and complete protection tool on the market. Various modules complement each other. The highly effective Anti-virus tool makes it difficult for harmful programs to install themselves and expose children to undesirable content. With Web Filter content control, the risk of downloading a virus is greatly reduced. If a virus does infect the machine, the Firewall, which controls activity, minimizes the harm that it can cause. Undesirable mail (or Spam) can be blocked with the Anti-spam service which uses Intelligent Multilanguage Content Analysis technology. The level of false positives is inferior to 0.4% and it is eliminated through the use of a quarantine module. Finally, the Anti-phishing service protects against phishing sites and Internet fraud, keeping personal data safe and confidential.

1.2 Main Features of Optenet Security Suite

- Over 99% effective in filtering.
- Error rate less than 0.1%, eliminated completely through the Contributions service.
- Integrates the most advanced technology: databases of websites, viruses and Spammers, Semantic Analysis Engine for online content and Spam blocking, heuristic analysis of executables, content-based protocol identification, etc.
- The filters do not affect communications; it takes less than a millisecond to analyze a web page.
- Automatic database and program updates.

- Reports on all filtering processes.
- Broad interpretation of the definition and nature of viruses, incorporating worms, trojans, spyware, adware, etc.

1.3 Optenet Security Suite Web Filter

Web Filter prevents access to undesirable Internet content, such as pornographic websites, dangerous file downloads, Instant Messaging servers or P2P.

It captures traffic entering and leaving the PC. In addition to identifying the type of traffic, it requests the relevant integrated service for analyzing, monitoring or tracing the content, ensuring that browsing is safe and based on the configured parameters.

It is based on semantic analysis of website content and lists of sites that have been placed in various content categories. The lists are updated every ten minutes. Independently of whether a website is included on a list, semantic analysis verifies whether the page contains any text with inappropriate content, in which case the User is blocked from accessing it.

1.4 Optenet Security Suite Anti-virus

Optenet Security Suite Anti-virus protects Users from viruses, spyware, trojans and worms that could infect their PC equipment through email or browsing the Internet, as well as detecting viruses already present on the computer.

Optenet Security Suite Anti-virus integrates latest generation virus detection technology developed by European company Kaspersky Lab. It offers various levels of protection. These levels allow the User to choose between preconfigured profiles. It is also possible to schedule scans or initiate them at any time.

1.5 Optenet Security Suite Anti-spam

The Optenet Security Suite Anti-spam protects Users from undesirable mail by using intelligent multilingual content analysis technology to block Spam. The level of false positives is less than 0.4% and is reduced to zero through the use of a quarantine module.

1.6 Optenet Security Suite Anti-phishing

Optenet Security Suite Anti-phishing protects Users from Internet fraud. It also provides complete protection of personal information such as passwords, credit card numbers, telephone numbers, addresses and other personal key information.

Protection is enforced by detecting fraudulent emails and by blocking sensitive information from being entered by mistake on phishing websites as well as reaching the Internet.

1.7 Optenet Security Suite Firewall

Optenet Security Suite Firewall controls the execution of applications that connect to the Internet. It is used to control connections, allowing Users to set the firewall to allow the connection, deny it or prompt the User each time an application initiates a connection. It also prevents unauthorized access to the User's PC, for example, by hackers.

Optenet Security Suite Firewall can be set to display an alert when a program attempts to connect to the Internet. The User can allow or deny the connection and can make the decision to take the default action whenever the program tries to connect.

1.8 Protocol Filtering

Protocol filtering detects connections and identifies the protocol type, performing various actions depending on the configuration. This allows Users to control applications like Instant Messenger, P2P, Chat, Email and Newsgroups.

1.9 Effectiveness

Optenet Security Suite leverages the most effective security service technologies. Content filtering uses a combination of the semantic analyzer and predefined lists giving the Security Suite an effectiveness of over 98%. The Anti-virus service achieves 99% effectiveness through integrated technology from Kaspersky.

Moreover, Optenet Security Suite's combination of filters makes its overall effectiveness far superior to that of each individual component.

For example, a piece of spyware could be blocked by any of the following mechanisms:

- Anti-virus detects spyware signatures.
- Anti-virus detects that the program is using techniques normally employed by spyware (heuristic analysis).
- The website hosting the spyware is in the database of the Web Filter, which blocks access to the page.
- The Web Filter content analyzer detects it as spyware.
- The administrator prohibits the download of executables as a preventative measure

1.10 Optenet Security Suite Languages

Optenet filters the main languages used on the Internet with over 98% effectiveness. The Security Suite lists contain pages from all languages. Additionally, the Semantic Analyzer is trained periodically with pages from around the world, enabling it to detect pages in all languages.

To achieve as high a level of effectiveness as possible (99%), for certain languages (e.g. English, Spanish, French, Dutch, Portuguese, German and Italian) a broad collection of pages is put together to train the Semantic Analyzer.

1.11 Browsing Speed When Using Optenet Security Suite

Optenet Security Suite is extremely fast and, as a result, is transparent to the User. Both the list query and the content analysis process performed by the system take one thousandth of a second. It is effectively an instantaneous process.

1.12 Web Filter Security

If attempts are made to get around the filter, Internet access is blocked completely as a security measure. Access can only be re-established using a password.

1.13 Unblocking Service for Pages Blocked in Error

Optenet Security Suite has an error rate of around 0.1%, the lowest on the market. In addition, it has an unblocking service. If a page is blocked in error, the User can automatically send an email to our Customer Care Center (CCC) explaining why the page should be unblocked. The User will be able to gain access to the page in around 15 minutes.

1.14 Activation or Deactivation of the Security Suite

Optenet Security Suite is activated or deactivated using a password so that administrators can browse without restrictions. The password is requested from the User at the time of installation. If the User does not have the password or if someone attempts to deactivate the Security Suite, the system has self-protection mechanisms that make it impossible to deactivate it.

1.15 Blocking P2P File Sharing and Downloading of Programs

It is possible to block P2P file sharing and downloading of programs through the protocol configuration of the Web Filter. The P2P server category can also be blocked, providing a greater level of security.

1.16 Blocking Instant Messaging Programs

It is possible to block Instant Messaging programs through the protocol configuration of the Web Filter. The Instant Messaging server category can also be blocked, providing a greater level of security.

1.17 Blocking Email

It is possible to block email through the protocol configuration of the Web Filter. To block webmail, the relevant category must be selected.

1.18 Updates

The list system is updated automatically via the Internet. This process requires no administration.



2 TECHNICAL REQUIREMENTS

2.1 Technical Knowledge

No specific technical knowledge is required to install or configure the filters.

2.2 System Compatibility

The OSSPC is available for the following operating systems:

- Windows XP Sp2
- Windows Vista (32 and 64 bits)
- Windows 7 (32 and 64 bits)

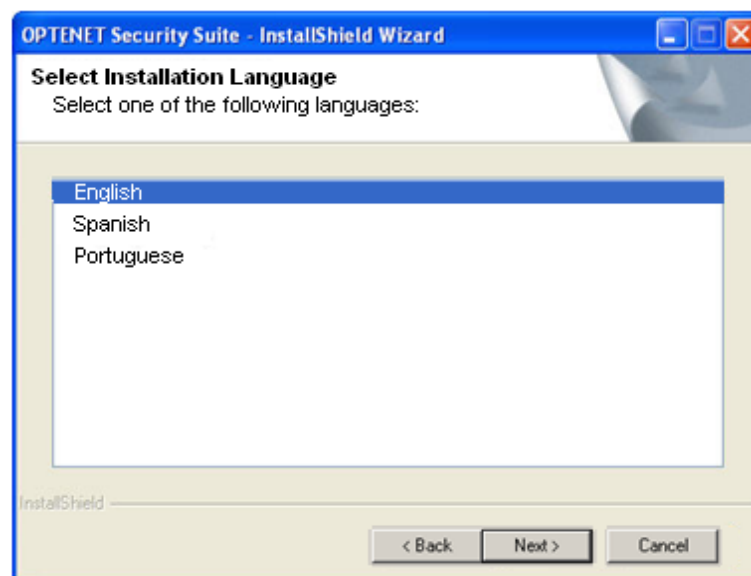
OS	RAM. Minumum:	Free Hard Disk Space:
Windows XP sp2	512 MB	200 MB
Windows Vista 32 bits, 64 bits	1 GB	200 MB
Windows 7 32 bits	1 GB	200 MB
Windows 7 64 bits	2 GB	200 MB

The system can be used with any Internet browser.

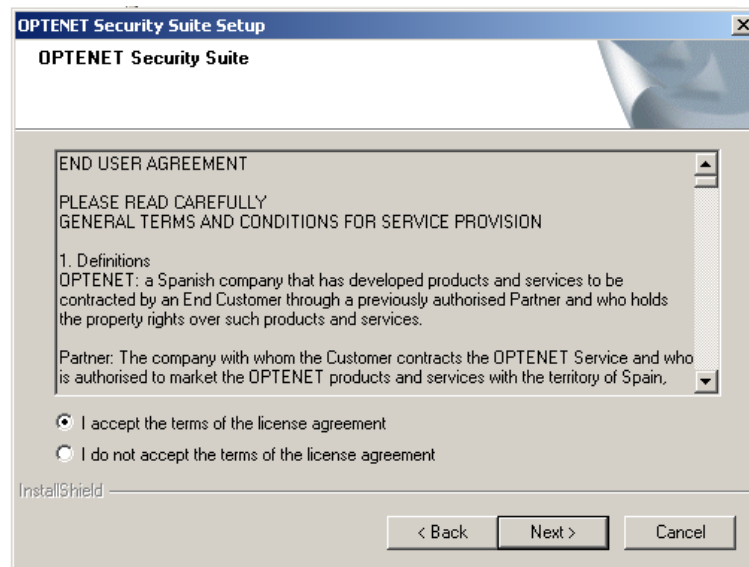
3 INSTALLATION PROCESS

Whether the tool is downloaded from the website or installed from a CD, it is recommended to save the program to the computer's hard disk and follow these steps:

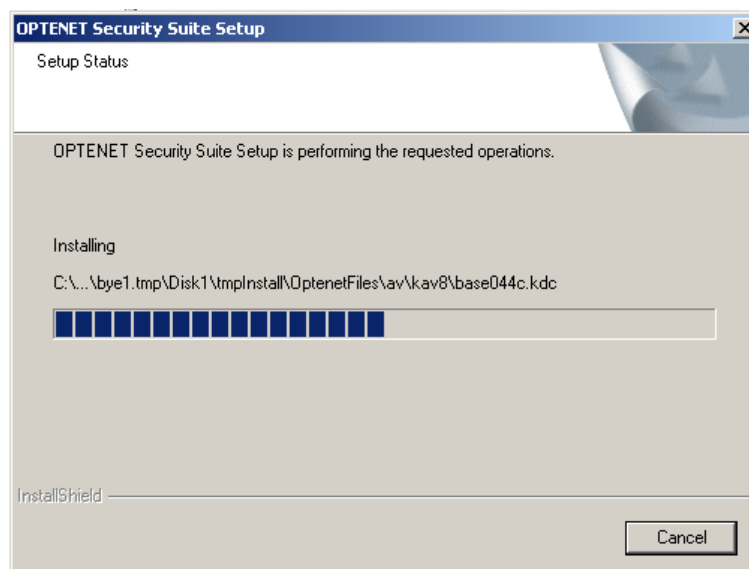
- 1) Double click on the file Optenet (the name of the file is OptenetSecuritySuite.exe)
- 2) The Optenet interface is available in three languages: Spanish, English and Portuguese. Select the language and click [Next].



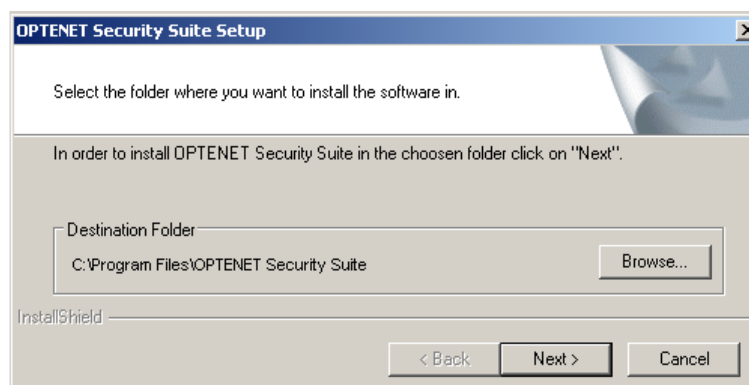
- 3) End User Agreement. Accept license terms:



- 4) Installation starts.



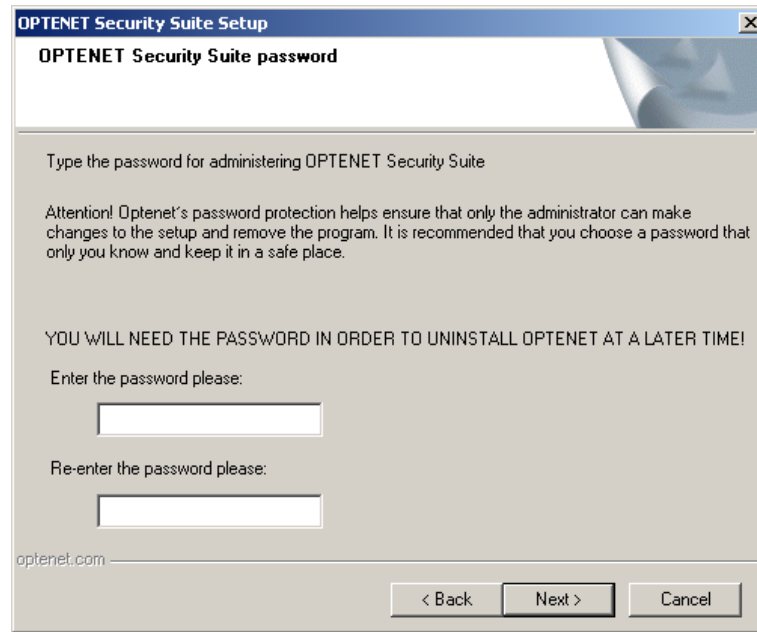
- 5) Select the folder where the software will be installed. By default, Program Files directory will be used. Click [Next].



- 6) Enter the password to be used to access the Optenet Administration Console (filter configuration).

This password ensures that only the administrator can make changes to the setup and remove the program. It is recommended that a password is chosen that is personal and confidential and should be kept in a safe place.

⚠ Remember that this password will be required to un-install Optenet Suite at a later time!



The screenshot shows a Windows-style dialog box titled "OPTENET Security Suite Setup". Below the title bar, the subtitle is "OPTENET Security Suite password". The main content area contains the following text:

Type the password for administering OPTENET Security Suite

Attention! Optenet's password protection helps ensure that only the administrator can make changes to the setup and remove the program. It is recommended that you choose a password that only you know and keep it in a safe place.

YOU WILL NEED THE PASSWORD IN ORDER TO UNINSTALL OPTENET AT A LATER TIME!

Enter the password please:

[Text input field]

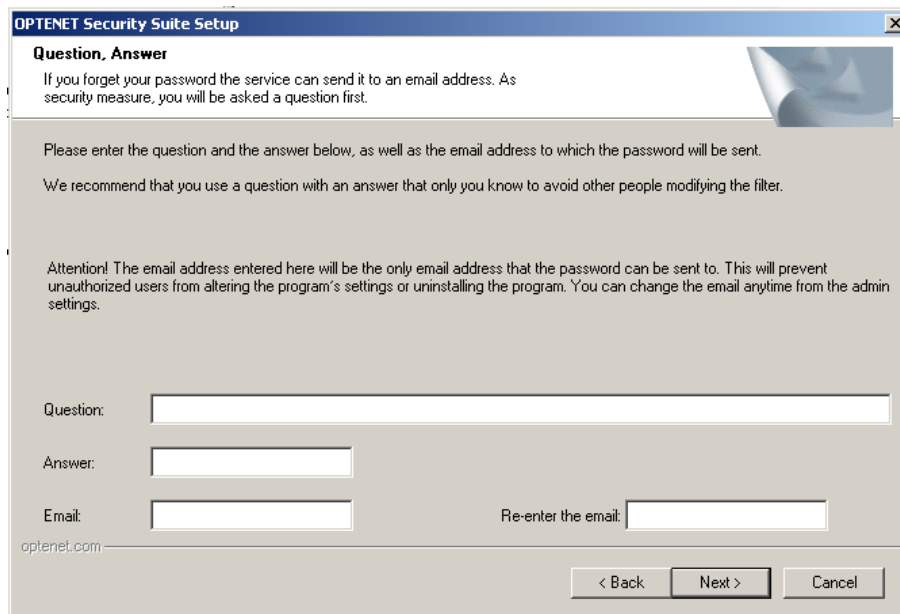
Re-enter the password please:

[Text input field]

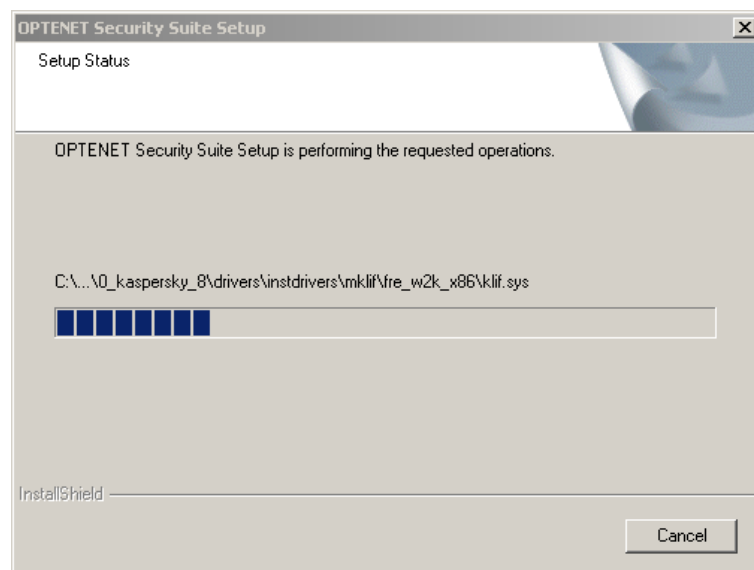
At the bottom left, the URL "opnet.com" is visible. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

- 7) Password Reminder:

- Type a question and answer to be used in case the password is forgotten.
- Enter an email address to send the password in case the configured control question has been forgotten. ⚠ The email address entered here will be the only email address where the password will be sent in case it has been! This will prevent unauthorized Users from acquiring the administrative password in order to alter filter settings and/or un-install the program.

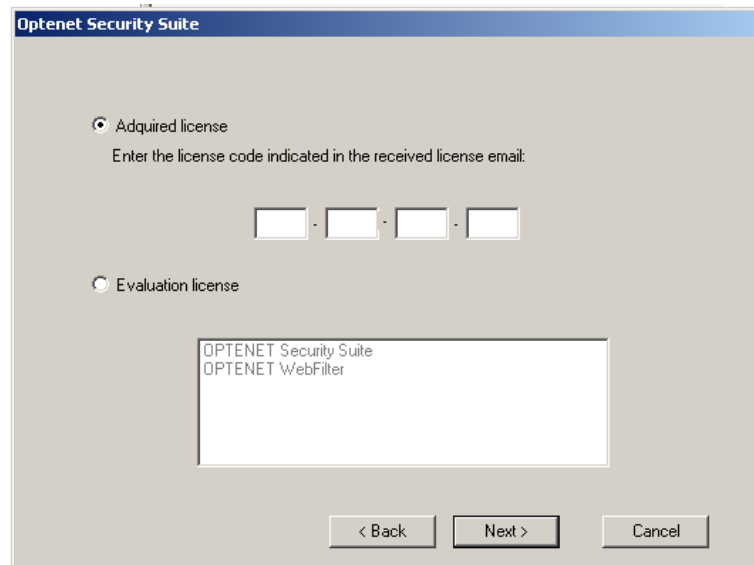


8) Installation starts...



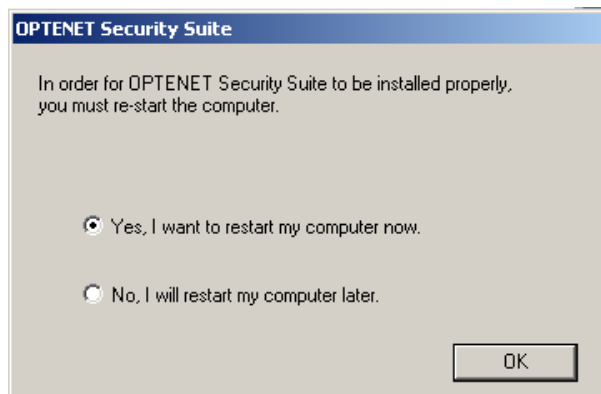
9) Enter license code (this will most likely have been received via email when the product was purchased).

Note: Where available, it may also be possible to use an evaluation license to try other available products (complete suite etc). In this case, select the trial Product and click on [Next].

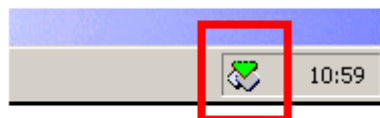


- 10) Finally, it is highly recommended to restart the PC to complete the installation.

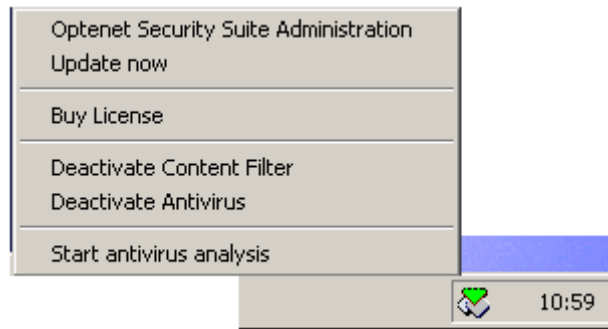
 The program may not work properly until the PC has been restarted.








- 11) Once the computer has been restarted, notice that a new icon is shown on Windows Status Bar.



Right-Click on it to open contextual menu (listed options might vary depending on installed product):



This icon will indicate filtering status or additional operations being performed at a given moment:

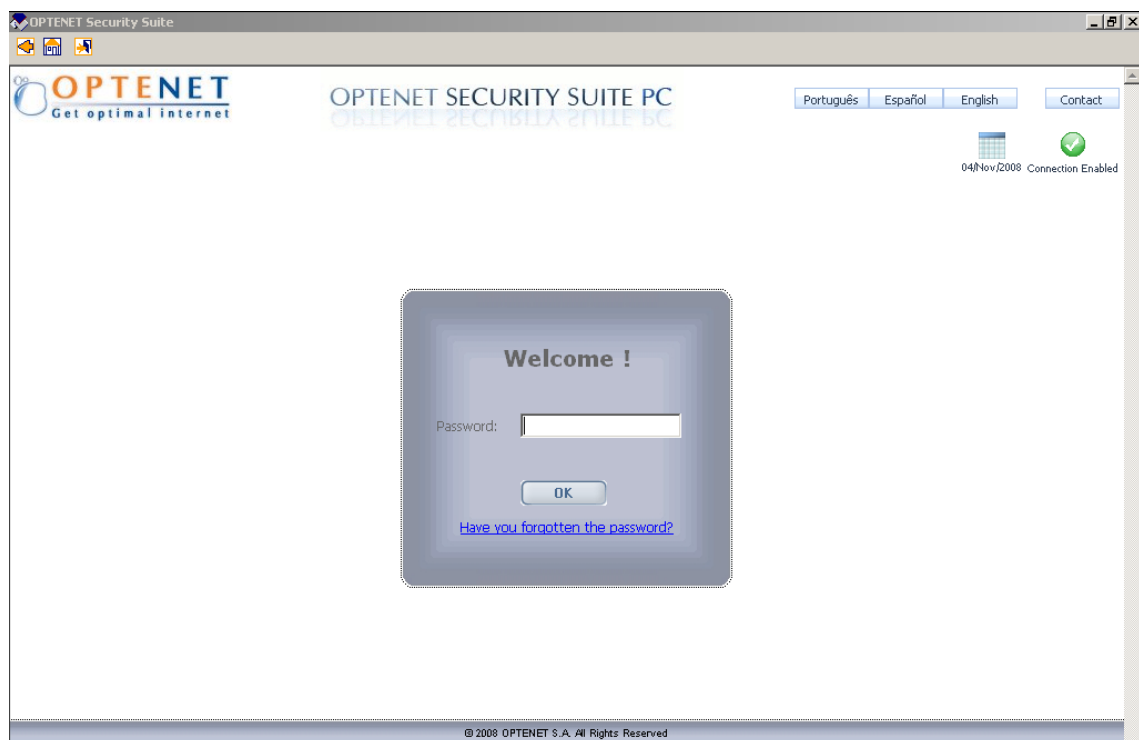
Icon	Meaning
	Filter Active
	Filter has been deactivated manually.
	Software or anti-virus signatures are being updated.
	Scanning for viruses
	License has expired. No filtering is being performed unless a license is acquired.

4 CONFIGURATION

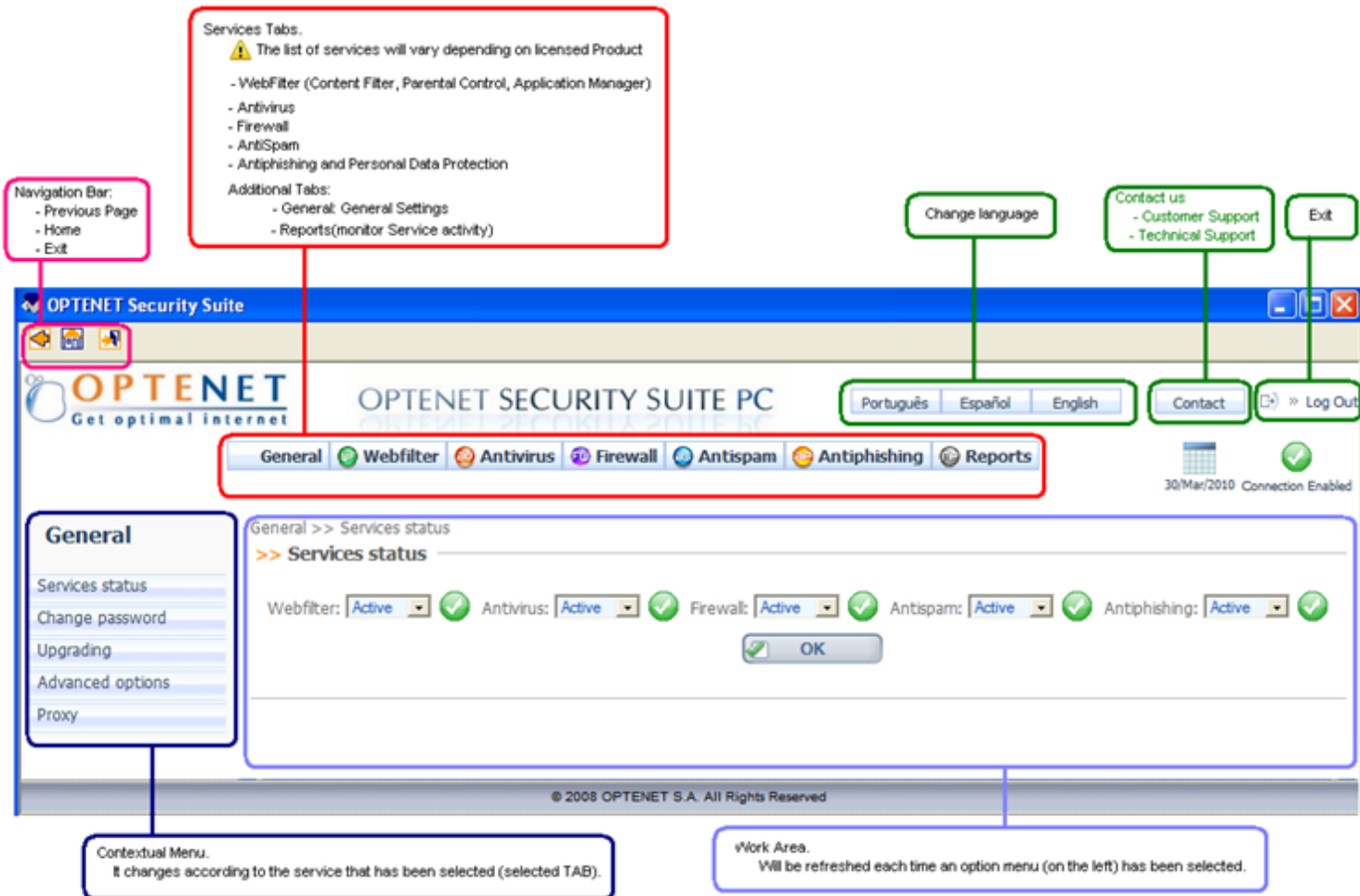
Optenet Security Suite Console can be accessed:

- From the Windows Start menu.
- Right-clicking on the Optenet icon on the windows status bar and selecting [Optenet Security Suite Administration].

An administrative password is required to prevent unauthorized access (this is the password indicated at installation time).



Once the password has been entered correctly, the administrative console will be shown:



Optenet Security Suite includes the following sections (when available, and depending on licensed product):

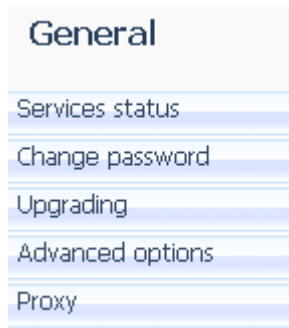
- General
- Web Filter
- Anti-virus
- Firewall
- Anti-spam
- Anti-phishing
- Reports

5 GENERAL

This section provides general information about the tool and the included services, and enables general configuration tasks such as:

- Enable/disable Services.
- Change administrative password.
- Configure software update.
- Change license code, configure a proxy (if required) etc.

When the *[General]* tab is clicked, this menu will be displayed on the left:

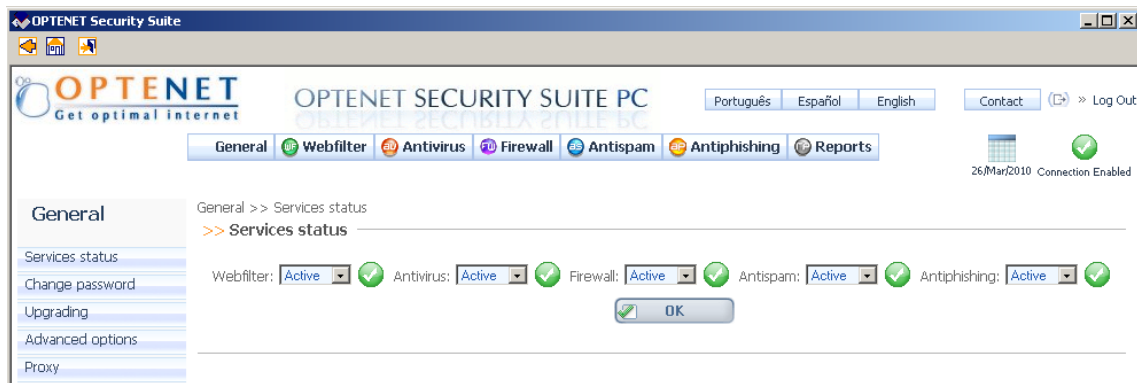


5.1 Service Status



Optenet Security Suite includes the following Services (depending on availability according to the product that is installed):


- Web Filter (parental control),
- Anti-virus,
- Firewall,
- Anti-spam
- Anti-phishing.

In this section, these services can be activated or deactivated:



There is a combo box enabling independently the activation/deactivation of each service. An icon indicates whether the service is currently active or not. If a service is not active, the configured filtering restrictions will not be applied.

Icon	Status
	Service is active
	Service is inactive

 Remember to click on [OK] button to apply changes.

5.2 Change Password

This section enables:

- The change of the administrative password.
- The change of the question/answer to be used in case the administrative password is forgotten.
- The change of the session lifetime.

General >> Change password

>> Change password

The password set here is used to access the filter configuration pages. You can also optionally add a question (or phrase) that will help you remember the password.

Current password: New password: Repeat the new password: 

OK

View details

>> Session lifetime (minutes)

Set the delay for the password to be requested again (admin session), avoiding the risk of unauthorized access using an open admin session.

Session lifetime (minutes):

(Elapsed time: 15)



OK

5.2.1 Changing the Administrative Password

This is for making changes to the password used to access the administration of the Optenet filter that was entered during the installation of the product.



Remember that this password prevents unauthorized access, so that filtering configuration can only be done by the administrator.

In order to change the password:

- Type current password.
- Type new password (and confirm it).

As an additional security measure, in case the administrative console is opened, it will be necessary to re-enter the administrative password periodically (by default, each 30 minutes). This measure avoids the risk of leaving the administrative console open enabling unauthorized Users to change the settings without the administrator's knowledge.

Enter the session lifetime (period before password is required to be re-entered in order to continue using the administrative console). Time expressed in minutes.

5.2.2 Changing Password Recovery Question/Answer and Email Address

General >> Change password

>> Change password

The password set here is used to access the filter configuration pages. You can also optionally add a question (or phrase) that will help you remember the password.



Current password:

New password:

Repeat the new password:



OK

View details

From the [Change Password] window, click on [View Details]. A new window will be opened where the password can be changed:

- The security question and answer. ⚠ Note: the answer is case sensitive.

And/or

- The email address.

General >> Change password >> View details

>> View details

-If you forget your password you will be shown this question and, if answered correctly, your password will be sent to the email address you configure here.

For example you could use --What's the name of my first cat?--, with the answer --Felix--. The answer is case-sensitive: Felix is not the same as felix, fElix etc.

Please note too that this question will be shown to anyone that attempts (and fails) to enter in the configuration pages. For this reason you should choose a question that only you know the answer to.-

Question:

Answer:

Email address:



OK

Back

Once these changes are saved, whenever the administrative password is requested, if it is forgotten, then click on the link below:



A new screen will appear asking for the Security question:

Password Reminder

Answer the password reminder and receive your password now

Question: **Day that I met my wife**

Answer:

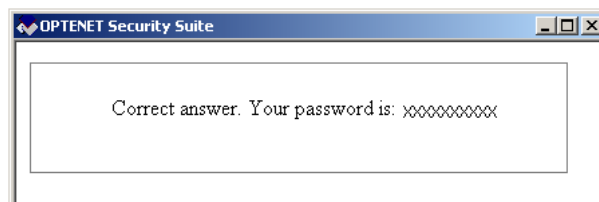
Proceed

Cannot remember the answer? The password will be emailed to your email account. **myaccount@myDomain.com**

Proceed

If you answer the question correctly your password will be sent to the email address you configured during the installation or the last time you changed your password.

- In the case where the answer is correct, a dialog will be displayed with the password.



- If not, the password will be sent to the email account defined during installation or the last time the password was changed.

5.3 Upgrading (Software Update)

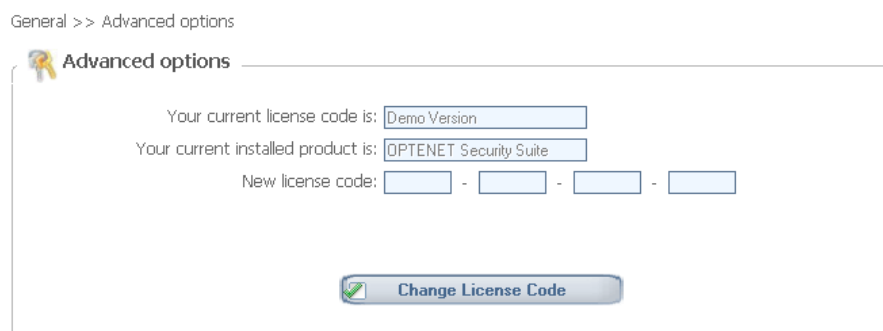
Optenet Security Suite can be updated automatically so the User does not have to worry about new versions. If automatic updates are not configured, Optenet Security Suite notifies the User when a new version of the software is available. The User can also update the software manually and in real time.

The type of alert to be used when a new version is available can be selected.



5.4 Advanced Options

This section allows the User to change the license code for the program.



5.5 Proxy Settings

In case there is no direct connection to Internet, this section enables the configuration of the proxy. In case the proxy requires authentication, enter the User and password to be used.

General >> Proxy

>> **Proxy**

Configure a proxy for Internet access

☒ Do not use a proxy

☐ Enter proxy configuration


Proxy HTTP: Port:

☐ Proxy needs authentication

User:

Password:

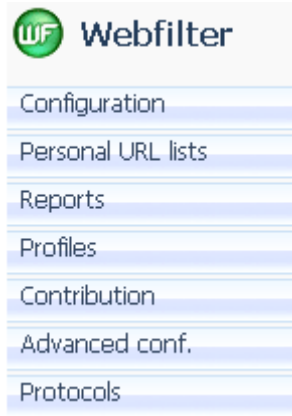
Retype Password:

 OK

6 WEB FILTER

This section enables Web Filtering to be configured (restrict the access to inappropriate web sites, the download of certain file types, etc).

When the [WebFilter] tab is clicked on, this menu will be displayed on the left:



6.1 Configuration

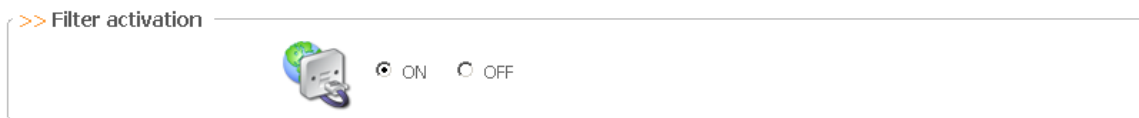
From the Web Filter configuration screen, it is simple to configure what Internet content Optenet Security Suite Users will be able to access.

The screen is divided in different sections:

- Filter status
- Unblock Internet access
- Categories to be filtered
- SafeSearch
- File types to be filtered
- Browsing schedules

6.1.1 Filter Status: Activate/Deactivate

The filter can be activated or deactivated as required:



- Inactive (**Off**): Users can access the Internet without restrictions.
- Active (**On**): Chosen categories are being filtered (restricted).

6.1.2 Internet blocked due to repeated attempts to access forbidden pages



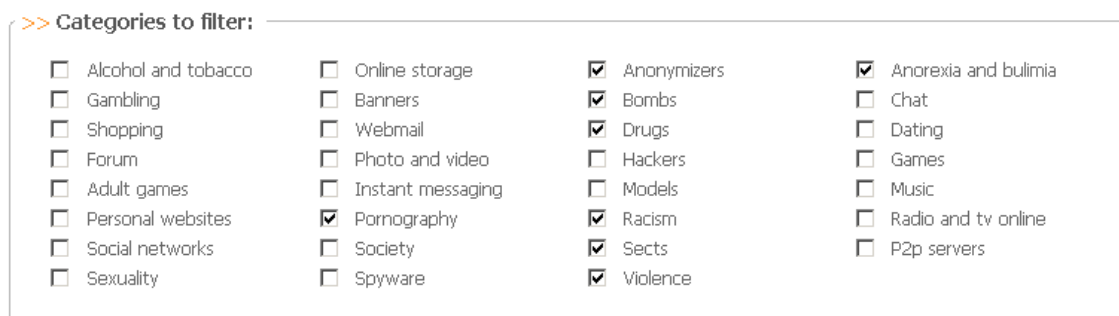
It is possible to block the access to Internet in case the User tries to access, during a single session, more than 10 forbidden pages. Mark the checkbox to activate this functionality.

- Only this User is blocked (not the rest of potential Users of the PC).
- To allow this User to navigate again, press on [*Unblock*] button.
- It is possible to configure an email address to receive a notification whenever this policy has been applied. The email will include:
 - » The User that has been blocked.

6.1.3 Selecting Web Categories to block

Select the categories to block. Web pages classified under these categories will be blocked.

By default, some categories are already marked:



Alcohol & Tobacco: Websites that sell or promote the use of tobacco or alcohol for human consumption, as well as items and products specifically related with its intake.

Gambling: Websites providing access to on-line casinos, bingo halls and on-line contests based on SMSs; this category includes websites where all kinds of bets can be placed and also offering training or actively promoting such activities

Shopping: Websites for online shopping of products or services. Sites allowing the offering and purchasing of goods between individuals or between an organization and an individual. It includes automobile shopping and real state agencies, even though no direct shopping is involved. It does not include gambling, travels and financial institutions.

Forums: Websites with a themed nature that invite you to participate with your personal opinions.

Adult games: Sites providing games of a violent, pornographic or erotic nature or content; also games related to hate, sects and racism. It includes multi-player open games where action might derive to such content.

Personal Websites: Personal websites created by Users all over the world in order to present themselves or present specific topics of interest to them.

Social Networks: Websites specifically devoted to setting up online communities where Users share information with each other. These sites might have a professional or entertaining purpose. This category excludes pages about dating and adult contacts.

Sexuality: Articles about sex, sex aimed at teenagers, sexual education etc., that do not contain pornography.

Online storage: Websites that offer Users the ability to store a large number of files, either as personal storage or sharing platform. This category does not include P2P.

Banners: Publicity or advertising banners inserted into websites. It includes sites serving them.

Web-mail: Websites where you can send and receive emails.

Photo & Video: Websites that host and allow the publication and viewing of images and/or videos. This category does not include professional and artistic photography.

Instant Messaging Servers: Websites from where you can download the programmes. It includes websites supporting SMS sending from the Internet.

Pornography: Websites with a pornographic or obscene content. It includes access to chat rooms where this type of material can be found.

Society: Websites with contents relating to celebrities; also content on fashion, décor, etc.

Spyware: Websites containing spyware. A spyware is a programme that recollects information from a PC to then transmit that information through the Internet to external sources. All this takes place without knowledge and/or consent of the PC owner.

Anonymizers: Websites that allow Users to browse the Internet and access Internet content without being registered by third parties.

Bombs (& Weapons): Websites that explain how to prepare, make, build, distribute and use explosives and explosive devices. Also sites that provide information, promote or sell firearms and sharp weapons for sport, hunting or military use; it does not include pocket and kitchen knives. In this category individuals or organizations that promote terrorism are also included. This category also includes pages related to the weapon, ammunition, and items for martial arts and personal defense (e.g. sprays, brass knuckles), including collector items.

Drugs: websites that encourage the use of drugs or provide contacts / places where drugs can be bought. It include sites directly selling prescription drugs without the supervision of a health professional. It does not include information / preventive measures about drugs.

Hackers: Websites where you can find illegal software as well as info in order to illegally gain access to information systems, hardware devices or personal equipments (cracking).

Models: Websites containing models' photographs; websites where this type of photograph shows models fully or partially naked are included in the pornography category.

Racism: Websites with contents of an openly xenophobic nature or which incite racist behaviour because of culture, race, sexual orientation, religion, ideology, etc.

Sects: Websites of dangerous sects, such as the so-called devil worshippers.

Violence: Websites whose contents are openly violent, that incite violence or defend it.

Anorexia and Bulimia: Websites devoted to promote and instigate eating disorders.

Chat: Websites where you can communicate with other Users in real time.

Dating: Websites through which you can meet other people: match-making, find a partner, etc.

Games: Websites where you can play on-line or download computer games.

Music: Websites where you can acquire or download music or get information about singers and groups in general.

Radio & TV Online: Websites of radio stations and TV channels. It includes those ones supporting on-line broadcasting.

P2P Servers: Websites that contain P2P applications and programs

6.1.4 SafeSearch

Select whether Google SafeSearch (and other Search Engines Search) is enabled. If this option is activated, all Google searches will be done with the SafeSearch option enabled (ignoring User settings for the Search Engine).

>> SafeSearch



☒ Active

Select this option to remove adult sites and sexually explicit content from Google search results.

6.1.5 File types to be filtered

In addition to filtering web pages, Optenet can place restrictions on the types of file that can be downloaded. The User can specify the file extensions that are to be blocked:

>> Files to filter


Not blocked:	Blocked
	
Shared Files: <input checked="" type="checkbox"/> ARJ <input checked="" type="checkbox"/> RAR <input checked="" type="checkbox"/> ZIP <input checked="" type="checkbox"/> CAB	Shared Files: <input type="checkbox"/> ARJ <input type="checkbox"/> RAR <input type="checkbox"/> ZIP <input type="checkbox"/> CAB
Images: <input checked="" type="checkbox"/> BMP (Microsoft Windows) <input checked="" type="checkbox"/> GIF <input checked="" type="checkbox"/> JPG (JPEG) <input checked="" type="checkbox"/> JPEG <input checked="" type="checkbox"/> PNG	Images: <input type="checkbox"/> BMP (Microsoft Windows) <input type="checkbox"/> GIF <input type="checkbox"/> JPG (JPEG) <input type="checkbox"/> JPEG <input type="checkbox"/> PNG
Music: <input checked="" type="checkbox"/> MP3 <input checked="" type="checkbox"/> OGG (Ogg Vorbis)	Music: <input type="checkbox"/> MP3 <input type="checkbox"/> OGG (Ogg Vorbis)
Programs: <input checked="" type="checkbox"/> BAT (Script MS-DOS) <input checked="" type="checkbox"/> CLASS (Java) <input checked="" type="checkbox"/> EXE (Microsoft Windows) <input checked="" type="checkbox"/> JS (Javascript) <input checked="" type="checkbox"/> PIF (Microsoft Windows) <input checked="" type="checkbox"/> VBS (Visual Basic Script) <input checked="" type="checkbox"/> SCR (Microsoft Windows Screen Saver) <input checked="" type="checkbox"/> COM (Microsoft Windows)	Programs: <input type="checkbox"/> BAT (Script MS-DOS) <input type="checkbox"/> CLASS (Java) <input type="checkbox"/> EXE (Microsoft Windows) <input type="checkbox"/> JS (Javascript) <input type="checkbox"/> PIF (Microsoft Windows) <input type="checkbox"/> VBS (Visual Basic Script) <input type="checkbox"/> SCR (Microsoft Windows Screen Saver) <input type="checkbox"/> COM (Microsoft Windows)
Video: <input checked="" type="checkbox"/> ASF (Microsoft Windows) <input checked="" type="checkbox"/> AVI (Microsoft Windows) <input checked="" type="checkbox"/> MOV (Apple Quicktime) <input checked="" type="checkbox"/> MPG (MPEG) <input checked="" type="checkbox"/> MPEG	Video: <input type="checkbox"/> ASF (Microsoft Windows) <input type="checkbox"/> AVI (Microsoft Windows) <input type="checkbox"/> MOV (Apple Quicktime) <input type="checkbox"/> MPG (MPEG) <input type="checkbox"/> MPEG
Other extensions:	
<div style="display: flex; align-items: center;"> <input style="width: 100px; height: 20px; border: 1px solid #ccc;" type="text"/> <div style="margin-left: 10px;"> <input type="button" value="Add >>"/> <input type="button" value="Remove <<"/> </div> </div>	

There are two lists:

- Files where download is permitted
- Files to block

By default, all file types are permitted.

In both lists, files are organized in “families”:

- Compressed Files
- Images
- Music
- Programs
- Video
- Custom extensions.  Note: at the bottom of the lists, there is a section where additional file extensions to block can be entered, making it possible to filter all file types.

Optenet filter uses “Content Analysis” to detect, for instance, MP3 files, even if they have been renamed with a different extension. For instance, if someone has renamed file queen.mp3 to queen.gif, the filter will detect and block it.

6.1.6 Browsing schedules

>> Surf schedule ☒ Active ☐ Inactive

Days	Intervals
Monday	<input type="text"/> to <input type="text"/> <input type="text"/> to <input type="text"/> <input type="text"/> to <input type="text"/>
Tuesday	18:00 to 20:00 <input type="text"/> to <input type="text"/> <input type="text"/> to <input type="text"/>
Wednesday	18:00 to 20:00 <input type="text"/> to <input type="text"/> <input type="text"/> to <input type="text"/>
Thursday	18:00 to 20:00 <input type="text"/> to <input type="text"/> <input type="text"/> to <input type="text"/>
Friday	18:00 to 20:00 <input type="text"/> to <input type="text"/> <input type="text"/> to <input type="text"/>
Saturday	10:00 to 11:00 16:00 to 17:00 <input type="text"/> to <input type="text"/>
Sunday	10:00 to 12:00 16:00 to 18:00 <input type="text"/> to <input type="text"/>



Example: 08:00-09:30 12:00-14:00 19:00-22:00 (You can configure up to three periods)

Enter the maximum number of hours with access to internet

Daily

Weekly


Internet access will be blocked upon reaching the configured time limit.

 Save Configuration  Restore Configuration

This section enables additional conditions to restrict the access to Internet to be established:


- If schedules are not activated, navigation will always be permitted (with the application of defined restrictions based on forbidden web categories and file types that can be downloaded).
- If schedules are activated, time limits for the use of Internet may be defined:

» Define up to three time periods per day of the week.

 Note: if no time period is set for a given day of the week, browsing will be permitted for the entire day (or until the maximum number of hours per day is reached).

» Maximum number of hours per day the User can navigate.

» Maximum number of hours per week the User can navigate.

 These options (Max. number of hours/day, Max. number of days/week) work independently of the time shown on the PC's clock.


Schedules can be activated or deactivated by checking the “**Active**” or “**Inactive**” options.

6.2 Personal URL lists (Black & White Lists)

Webfilter >> Personal URL lists

>> Personal URL lists

Adding a URL to the lists on this page allows you to override the normal treatment of a given web page:




Allowed web pages

Only the exact address* ☐

Add

Delete



Blocked web pages

Only the exact address* ☐

Add

Delete

* If you select this option, the filter will only block this exact Web page (e.g. www.yahoo.com). If not, it will block this Web page and all the pages on this web server too (e.g. www.yahoo.com, www.yahoo.com/mail, www.yahoo.com/shopping etc.).

It is possible to create a White list of trusted URLs and a black list of URLs to block regardless of the category they belong to:

- The filter can be customized so that specific pages from “prohibited” categories can still be viewed when the filter is active. These are known as Allowed Web Pages.
- In a similar way, Users can be prevented from viewing certain pages, regardless of the category the pages belong to.

- To allow or block a single web page, check the option “Only the exact address”.
- If not, the whole domain will be blocked.
 - » Eg. If www.yahoo.com is entered and “only the exact address” is not checked, the following sub-domains will be blocked or permitted too:
 - ♦ www.yahoo.com/mail
 - ♦ www.yahoo.com/shopping etc

6.3 Reports (Browsing history)

Reports on pages that Users have tried to access and whether they were blocked or not. Reports only show information related to navigation while the filter has been active.

In this section, it is possible to:

- Decide whether to save information about browsing attempts.
 - » Mark the checkbox [Save reports] to log this information.
 - » Decide the frequency of the deletion of browsing history files (in order to save disk space). By default this is set to 15 days.
- View navigation history (information available where [Save reports] option has been checked).

Webfilter >> Reports

>> Reports configuration

☒ Save reportsReport files will be deleted each days Accept

>> View reports


 View reports

Click on [View Reports] to define:

- Time range (from date to date)
- Number of lines to show (number of http requests to show):

Web filter >> Reports

>> Reports

Start date: / / Start hour: End date: / / End hour: Number of lines to show:  Show

>> Reports:

```

general 07/Jul/2008:10:10:17 http://secure-uk.mir.worlwide.com/cgi-bin/m?ci=es-actualidadg-bacc=rami=shing=ccor=AWAAR07MPC 1
bannerspyware html
general 07/Jul/2008:10:18:18 http://ad.es.doubleclick.net/adi/N5256.elmundo/B2982490;sz=728x90;ord=12154186212030139298? 1
bannerspyware html
general 07/Jul/2008:10:18:18 http://ad.es.doubleclick.net/adi/N5256.elmundo/B2982490;sz=728x90;ord=12154186212030139298? 1
bannerspyware html
general 07/Jul/2008:10:18:18 http://www.elmundo.es/cajas/espana/06/contador.txt 1 press txt
general 07/Jul/2008:10:18:18 http://estaticos03.cache.el-mundo.net/elmundo/iconos/tiempo/sol.png 1 bannerspress png
general 07/Jul/2008:10:18:18 http://ad.es.doubleclick.net/adi/N5132.elmundo.mecinteration/B2972072.2;sz=300x250;ord=12154186212030139311? 1
bannerspyware 2
general 07/Jul/2008:10:18:42 http://www.playboy.com/ 0 modelspornographypress html
david 07/Jul/2008:16:24:05 http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome 1 - dll
david 07/Jul/2008:16:24:06 http://go.microsoft.com/fwlink/?LinkId=54729&clcid=0x040a 1 kids html
david 07/Jul/2008:16:24:06 http://es.msn.com/ 1 portals html

```

Back

The report lines follow this format:

profile name	date	time	URL	not blocked (0)/blocked (1)	category	file type
--------------	------	------	-----	-----------------------------	----------	-----------


6.4 Filtering Profiles

When different Users operate on the same PC, different rules for each User or set of Users should probably be defined.

Eg. Defining different restrictions for a 10-year old child, a 16-year old child and for a parent or adult.

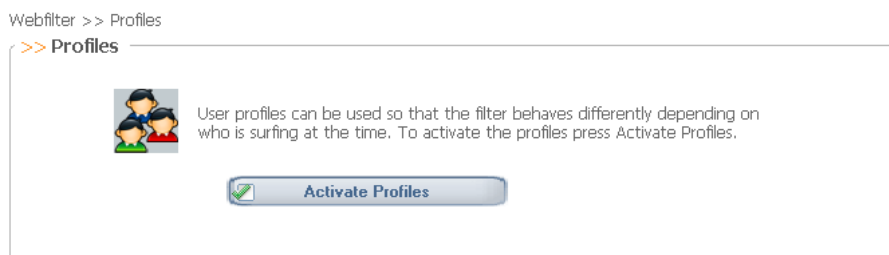
A filtering profile enables the filter to operate differently to the default settings and is only applied to certain Users.

If no new profiles are created, the filter operates with the default configuration described above.

 The administrator can provide each member of a family/company with an individual filtering profile based on, for example, their age or position.

If profiles are enabled, when Users try to establish an Internet connection, they are required to authenticate against one of the defined profiles.

6.4.1 Enabling/Disabling the use of Profiles



Profiles are filtering modes customized according to who is browsing. Profiles are commonly used when a PC has more than one User. For example, in families it is normal to set up different profiles for children and adults.

To activate filtering profiles:

- 1) Access the filter administration menu.
- 2) Select the Web Filter tab.
- 3) Choose the Profiles option.
- 4) Click on [Activate Profiles].

If no special measures are required and all Users are to be treated in the same way by the filter, existing profiles can be disabled. This is only possible if profiles were previously defined and enabled. To disable filtering profiles:


- 1) Access the filter administration menu.
- 2) Choose the Profiles option.
- 3) Click on [Deactivate Profiles].

From now on, all Users will navigate using the default filter configuration

6.4.2 Creating a new profile

Webfilter >> Profiles

>> Profiles

 Press this button to deactivate user profiles. Once deactivated, all users will use the same general profile.

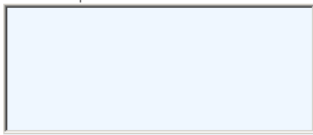
[Deactivate profiles](#)

To create a new profile, you must enter a user name and a password. A valid profile name may not include either spaces or punctuation marks, except the underline character (_).

New profile:

[New profile](#)

To modify the profile's configuration, or to delete or change the profile's password, choose a profile name and press the correct button.



[Modify configuration](#)

[Delete profile](#)

To create a filtering profile:

- 1) Access the filter administration menu.
- 2) Select the Web Filter tab.
- 3) Choose the Profiles option.
- 4) Click on Activate Profiles.
- 5) Enter the profile name in the New Profile box.
- 6) The name of the profile created will appear in the bottom box.

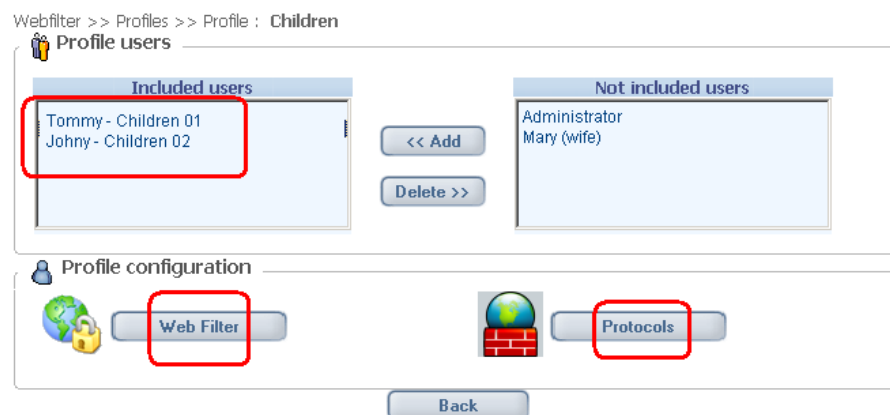
6.4.3 Configuring/Editing a profile

To configure or modify a filtering profile:

- 1) Access the filter administration menu.
- 2) Select the Web Filter tab.
- 3) Choose the Profiles option.
- 4) Select the profile to be modified or configured.
- 5) Click on [Modify configuration].
- 6) A new screen appears with the name of the profile that is being modified displayed at the top.
- 7) The profile appears empty if it has just been created. Otherwise the last saved configuration is displayed. When a new profile is created, it must be configured otherwise by default it will be empty.



First, Users that will be included in the profile must be selected. The list of available Users in the computer is shown:



Then, for the active profile the following can be configured:

- Web Filtering restrictions (categories, files to block, navigation schedules etc).
- Protocol restrictions (restrictions based on application protocols: P2P, instant messenger, Email, Newsgroups, chat, virtual worlds, others).

Specific Web Filter Restrictions:

Click on [Web Filter]. A new window is opened in order to configure the filtering restrictions for this profile.

Click on [Use General Configuration] to copy general settings. This profile can then be configured, adding or removing restrictions:

Webfilter >> Profiles >> Profile : Children

>> Profiles



Use general configuration



Show profile URL lists

>> Categories to filter:

- | | | | |
|--|---|---|--|
| <input type="checkbox"/> Alcohol and tobacco | <input type="checkbox"/> Online storage | <input checked="" type="checkbox"/> Anonymizers | <input checked="" type="checkbox"/> Anorexia and bulimia |
| <input type="checkbox"/> Gambling | <input type="checkbox"/> Banners | <input checked="" type="checkbox"/> Bombs | <input type="checkbox"/> Chat |
| <input type="checkbox"/> Shopping | <input type="checkbox"/> Webmail | <input checked="" type="checkbox"/> Drugs | <input type="checkbox"/> Dating |
| <input type="checkbox"/> Forum | <input type="checkbox"/> Photo and video | <input type="checkbox"/> Hackers | <input type="checkbox"/> Games |
| <input type="checkbox"/> Adult games | <input type="checkbox"/> Instant messaging | <input type="checkbox"/> Models | <input type="checkbox"/> Music |
| <input type="checkbox"/> Personal websites | <input checked="" type="checkbox"/> Pornography | <input checked="" type="checkbox"/> Racism | <input type="checkbox"/> Radio and tv online |
| <input type="checkbox"/> Social networks | <input type="checkbox"/> Society | <input checked="" type="checkbox"/> Sects | <input type="checkbox"/> P2p servers |
| <input type="checkbox"/> Sexuality | <input type="checkbox"/> Spyware | <input checked="" type="checkbox"/> Violence | |

>> Files to filter

Not blocked:

Blocked

Click on *[Show Profile URL lists]* to open a window where a specific white list and black list of urls can be defined for this profile:

... >> Personal URL lists >> Personal URL lists: Children

>> Personal URL lists

Adding a URL to the lists on this page allows you to override the normal treatment of a given web page for this profile.



Allowed web pages



Blocked web pages

Only the exact address* ☐

Add



Delete

Only the exact address* ☐

Add

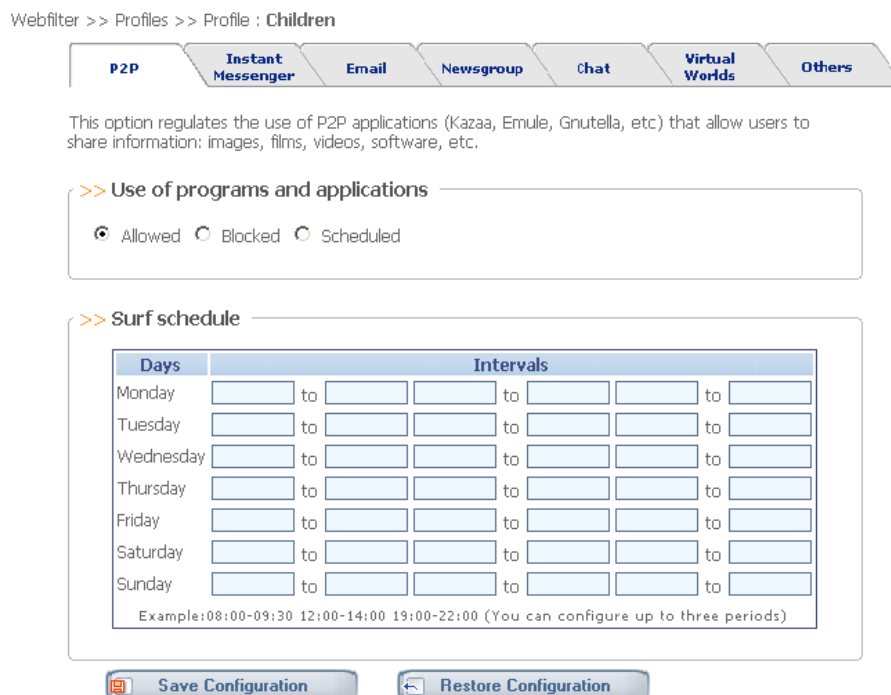


Delete

Specific restrictions based on application protocols:



Click on [Protocols]. A new window is opened in order to configure the filtering restrictions for this profile:



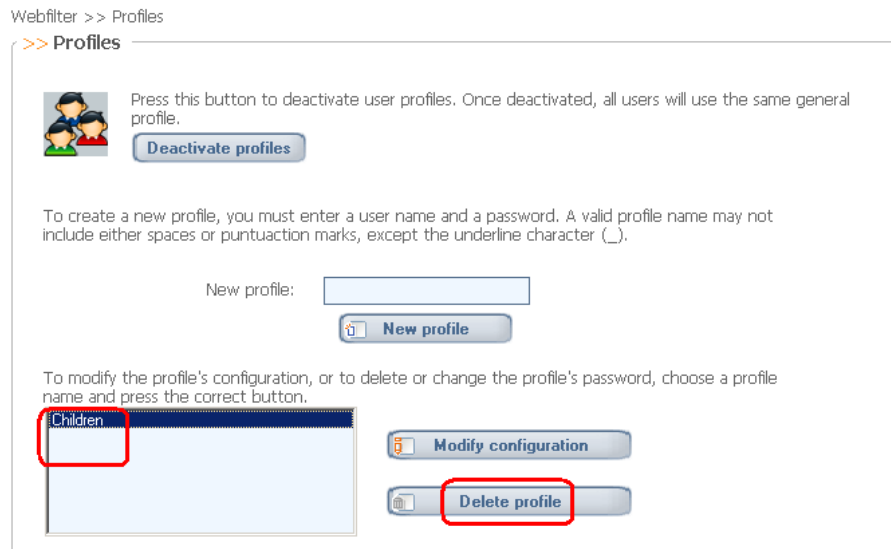
Protocol restrictions will be described later in this manual.

6.4.4 Deleting a filtering profile

To delete a filtering profile:

- 1) Access the filter administration menu.
- 2) Select the Web Filter tab.
- 3) Choose the Profiles option.
- 4) Select the profile to be deleted.

5) Click Delete profile.



6.5 Contribution – Add Websites to the filter

Contribute with addresses of Internet pages that are not being detected by the filter (a url not included in Optenet lists nor detected by content analysis) but which should be considered to be included as part of any of the web categories (porn webpages etc).

Optenet's Review department checks the contributed addresses and assigns them to the appropriate category.

When a page has been reviewed, it is placed in one of the filtering categories. Additionally, if Users provide their email address, they are informed of what action has been taken regarding their request.

In contrast to the Personal Lists, the Contribution function is used to inform Optenet of a page that should be filtered, to the benefit of all Users of the filter.



OPTENET SECURITY SUITE PC

Add websites to the filter

[Contact](#)
[Close](#)

If you think this website page should be restricted you can let us know writing the address of the page in "Website" and clicking on "Send"

If you like, you can give us your e-mail address and Optenet will send you confirmation when the website has been analysed.

E-mail address (optional):

Web page address:

Observations:

6.6 Advanced Configuration

The web pages that are added to this list will not be filtered and will not appear in the browsing history. Access will always be allowed to these pages or servers.

Simply add the names of the automatic update servers, for example, the website used to update the Anti-virus.

Once these changes have been made, the computer must be restarted in order for the changes to take effect.

The pages entered in this section are completely excluded from filtering. They will not appear in the browsing history, they will never be blocked and they are exempt from browsing schedules.

Webfilter >> Advanced conf.

>> Advanced conf.



The options available on this page are advanced configuration options, and should not be modified unless absolutely necessary. If you are in any doubt as to whether or not you should change the settings shown here please contact our Client Support Service.



Excluded Web Servers

The server URLs that you add to this list will not appear in the navigation history, nor will they be filtered. If you have profiles activated these servers will not trigger the profile authentication window.

Typically you should only add automatic updating servers to these lists, for example the url used for antivirus updates, Windows updates etc.

Note that you should only add the first part of the URL. For example, if the URL shown in the navigation history were

`http://cache511ss.optenet.com/gettrans.dll?id=xa1` you should only add --

`cache511ss.optenet.com--.`

Any changes made here will only take effect after restarting your machine.

Excluded Web Servers





6.7 Protocol filtering

In this section, the different application protocols to be filtered can be configured by selecting the action that should be taken with each one:

- Allowed – access to the programs and applications for that protocol category is permitted.
- Blocked – access to the programs and applications for that protocol category is blocked.
- Scheduled – access is regulated by time, depending on the timeframes specified in the Surf Schedule table:
 - » On the days where a timeframe is specified, access will be permitted only on those timeframes.
 - » On the days where a timeframe is not specified, access will be permitted the entire day.

The defined protocols are:

- P2P
- Instant Messaging
- Email
- Newsgroups
- Chat
- Virtual worlds
- Port configuration (others).

Web filter >> Protocols



This option regulates the use of P2P applications (Kazaa, Emule, Gnutella, etc.) that allow users to share information: images, films, videos, software, etc.

>> Use of programs and applications

☐ Allowed ☒ Blocked ☐ Scheduled

>> Surf schedule

Days	Intervals					
Monday	<input type="text"/>	to	<input type="text"/>	<input type="text"/>	to	<input type="text"/>
Tuesday	<input type="text"/>	to	<input type="text"/>	<input type="text"/>	to	<input type="text"/>
Wednesday	<input type="text"/>	to	<input type="text"/>	<input type="text"/>	to	<input type="text"/>
Thursday	<input type="text"/>	to	<input type="text"/>	<input type="text"/>	to	<input type="text"/>
Friday	<input type="text"/>	to	<input type="text"/>	<input type="text"/>	to	<input type="text"/>
Saturday	<input type="text"/>	to	<input type="text"/>	<input type="text"/>	to	<input type="text"/>
Sunday	<input type="text"/>	to	<input type="text"/>	<input type="text"/>	to	<input type="text"/>

Example: 08:00-09:30 12:00-14:00 19:00-22:00 (You can configure up to three periods)

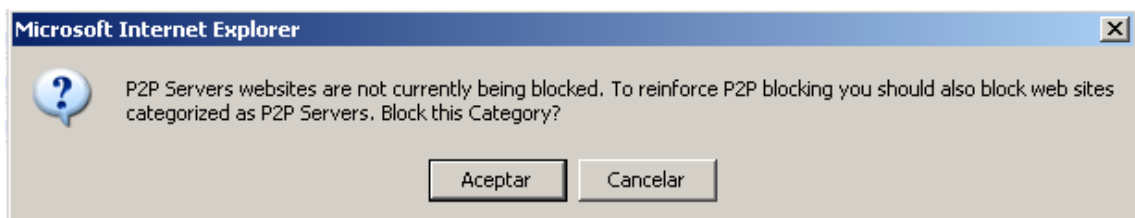
Save Configuration

Restore Configuration

6.7.1 P2P

This option is used to control the use of P2P applications (e.g. Emule, Gnutella, Kazaa) used to share pictures, films, videos, software, etc.

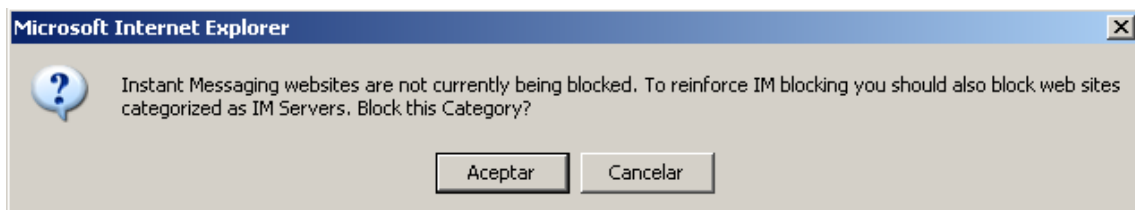
⚠ Where P2P protocols are set to be blocked, if the web category “P2P Servers” is not being blocked (see [WebFilter >> Configuration]), the program will also request these types of websites to be blocked:



6.7.2 Instant Messaging

This option is used to control the use of Instant Messaging applications (e.g. Microsoft MSN Messenger, Yahoo Instant Messenger, ICQ 5.0, AIM), used to send messages and share files in real time.

⚠ Where IM protocols are set to be blocked, if the web category “Instant Messaging Servers” is not being blocked (see [WebFilter >> Configuration]), the program will also request these types of websites to be blocked:

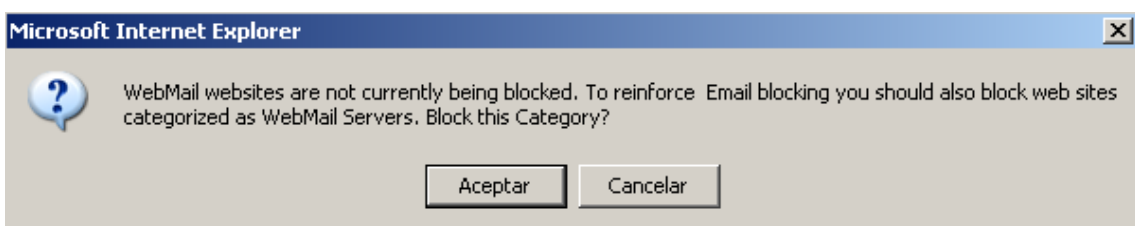


6.7.3 Email

This option is used to control the use of email accessed through the protocols POP3 (port 110), SMTP (port 25) and IMAP (port 143).

To filter access to webmail, select this category when configuring which categories to filter.

⚠ Where email protocols are set to be blocked, if the web category “Web Mail websites” is not being blocked (see [WebFilter >> Configuration]), the program will also request these types of websites to be blocked:




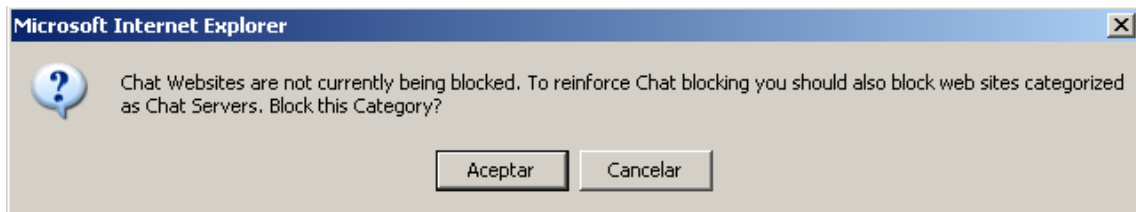
6.7.4 Newsgroups

This option is used to control the use of newsgroups (e.g. NNTP), used as discussion forums where Users can exchange opinions.

6.7.5 Chat

This option is used to control the use of chat applications (e.g. IRC), through which Users communicate with each other.

 Where Chat protocols are set to be blocked, if the web category “Chat” is not being blocked (see [WebFilter >> Configuration]), the program will also request these types of websites to be blocked:

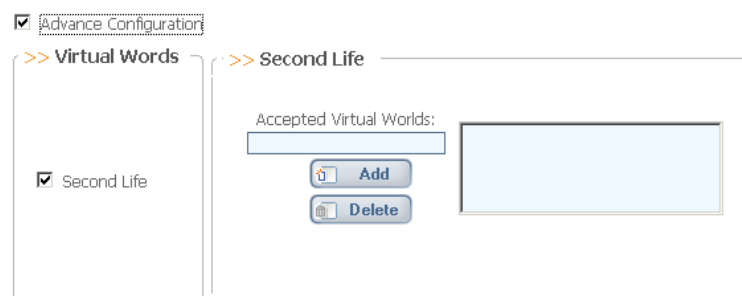


6.7.6 Virtual Worlds

This option is used to control the use of Internet-based virtual world games (such as Second Life) where Users can inhabit and interact via avatars.

Additionally, by enabling the Advanced configuration checkbox, a list of exceptions with URLs/addresses can be configured to allow or block access, as follows:

- » Use of virtual worlds is allowed and there are no addresses in the advanced configuration list: access is allowed to all addresses in the virtual world.
- » Use of virtual worlds is blocked and there are no addresses in the advanced configuration list: access is blocked to all addresses in the virtual world.
- » Use of virtual worlds is allowed and addresses present in the advanced configuration list: access is only allowed to the addresses in the list.
- » Use of virtual worlds is blocked and addresses present in the advanced configuration list: access is blocked to all addresses in the list.



6.7.7 Other

This option is used to define the default behavior (access blocked or allowed) for all other ports not included in the configuration of the previous tabs. In either case, exceptions to the above rule can be defined by entering specific ports or range of ports to be blocked or allowed, as applicable.

Web filter >> Protocols



This option blocks or allows access to all other ports not included under the previous headings. To establish exceptions enter the ports you wish to permit or block below:

☐ Block all other ports
Exceptions:

☒ Allow all other ports
Exceptions:

6.8 Reinforcing the blocking

Sometimes, there is a similarity between web categories and families of protocols:

Protocol	Web Category
P2P	P2P Servers
Instant Messaging	Instant Messaging
Email	WebMail
Chat	Chat
etc	

For this reason, whenever the filter is configured to block any of these web categories, the program will ask if related protocols are to be blocked to reinforce the blocking (if those protocols are not set to be blocked yet).

In a similar way, whenever a given protocol is blocked, if the similar web category is not being blocked, the program will ask if related websites should also be blocked.

Eg: If a given profile should not use applications based on email protocols, the program will ask if webmail sites for this profile should be blocked.

7 ANTI-VIRUS

Optenet Security Suite includes its own Anti-virus tool with a complete range of functionality.

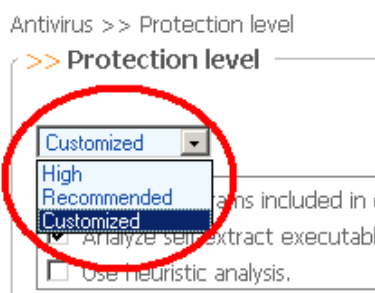
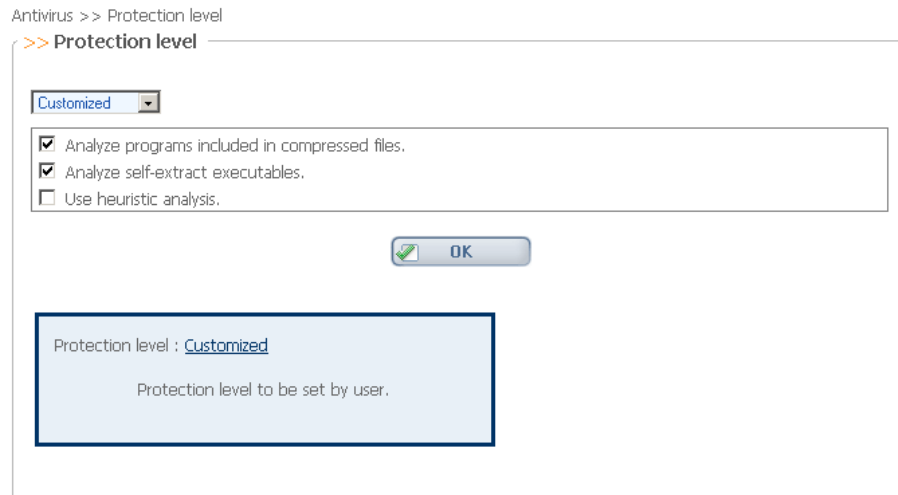
This section enables the configuration of malware detection.

When the [Anti-virus] tab is clicked, this menu will be displayed on the left:



7.1 Protection Level

In the Optenet Security Suite Anti-virus section, the level of protection for the computer can be configured.



The available levels of protection are:

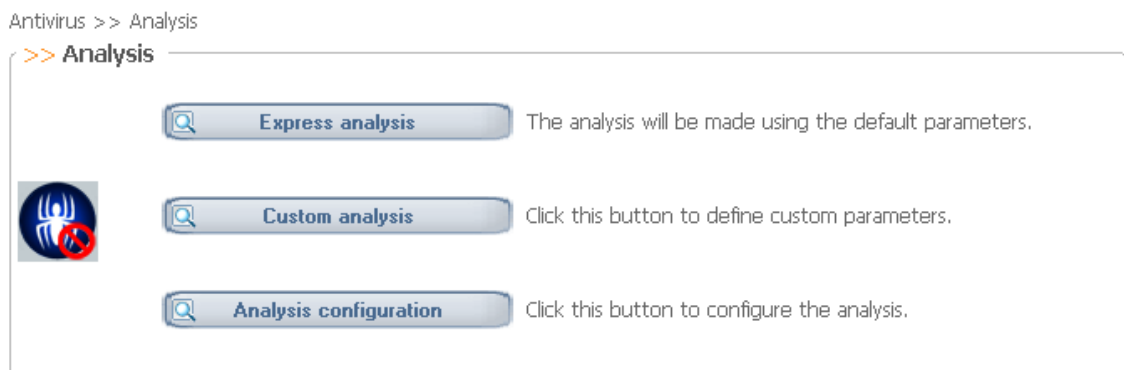
- High
- Recommended
- Customized.

Only where the “Customized” mode is selected, the User can fine-tune the behavior of the Anti-virus (Anti-virus techniques and files to be analyzed):

- Analyze programs included in compressed files
- Analyze self-extract executables.
- Use heuristic analysis

7.2 Analysis

In this section, the Anti-virus can be launched and an analysis performed, based on the default parameters, and custom settings for the analysis can be configured.



The Anti-virus can analyze all PC units and memory.

Click on [Analysis configuration] to open a new window and define default settings:

Antivirus >> Analysis >> Analysis configuration

What elements do you want to analyze?☒ **Memory**When virus found Quarantine infected process.When suspicious found Quarantine infected process.☒ **File System**When virus found Quarantine infected file.When suspicious found Quarantine infected file.**Elements to analyze:**☒ Whole computer

- ☒ Analyze hard disks
- ☒ Analyze floppy drives
- ☒ Analyze CDROM/DVD drives
- ☒ Analyze USB drives

☐ Folders or Drives.☐ Analyze elements by file extension>> **Elements to except from analysis:**

Elements to except from analysis:

Select Files.

Drive/Folder:

Search SelectAddRemove>> **Schedule****Configure programmed analysis**

- ☐ Don't perform programmed analysis.
- ☒ Daily analyze at 09 : 30 Hours
- ☐ Weekly analyze Monday at 09 : 30 Hours

Memory Analysis:

Decide whether memory analysis has to be performed.

If a virus is found while scanning the memory, one of the following measures can be taken:

- Alert that a virus has been found.
- Kill the infected process.
- Quarantine the infected Process.

In a similar way, a decision can be made on what to do with a suspicious virus that has been found.

File System Analysis:

A decision can be made on what to do whenever an infected file or suspicious virus has been found.

Configure the units that will be analyzed by default:

- The whole PC
- Just some units according to their types:
 - » Hard Disks
 - » Floppy drives
 - » CDROM/DVD Drives
 - » USB drives
- Some folders and drives. A new window will be shown to select the folders and/or drives to be analyzed:

>> Drives

Drives:	Folders:	Files:
<div>...</div> <div>Set Drive</div> <div>Set Folder</div> <div>OK</div>		

- Optionally, files to be analyzed according to their types (compressed files, music files, programs ...) can also be indicated.

Exceptions

Indicate drives or folder that will not be analyzed.

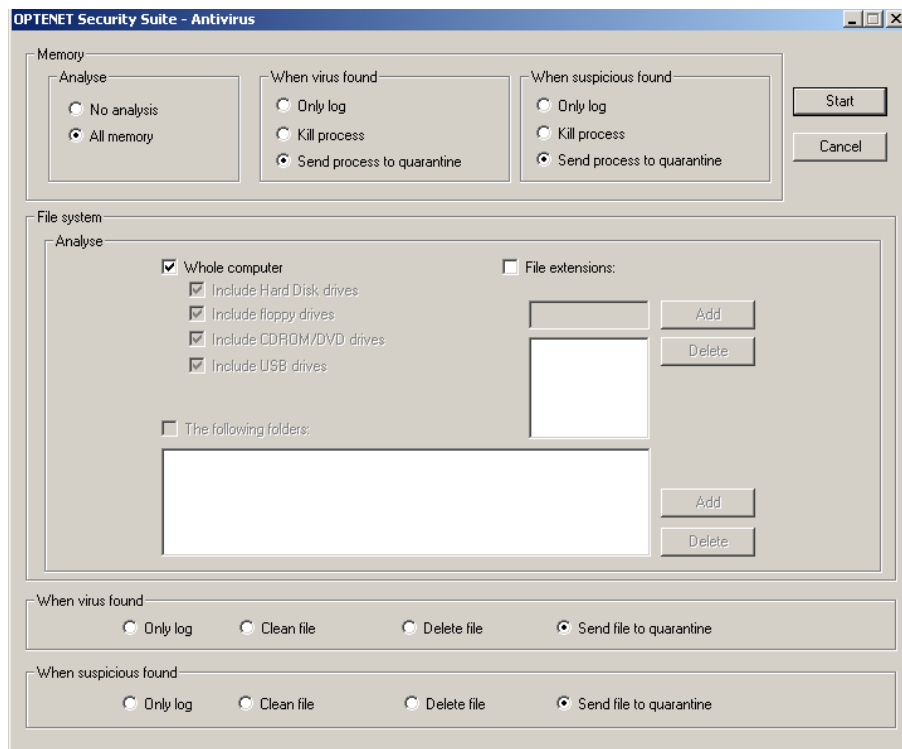
Scheduling the analysis

It is possible to configure programmed analysis (with the settings defined before).

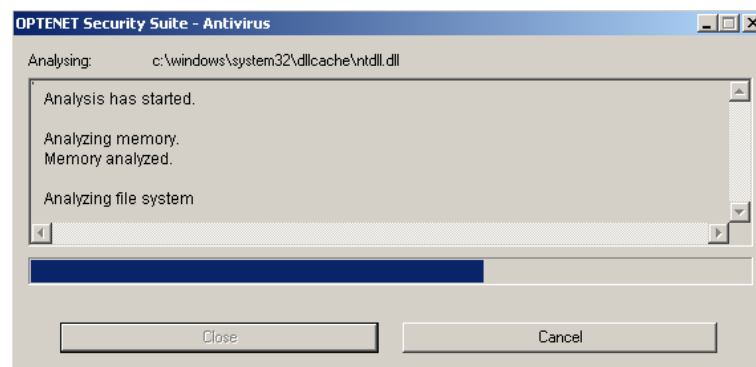
Options:

- Do not perform programmed analysis
- Daily at a given hour
- Weekly at a given day and hour

Click on **[Custom Analysis]** to scan for viruses at this moment without modifying default analysis settings. A new window will be opened in order to configure current analysis:



Start the analysis. A new window will show the evolution of the analysis:



Click on [**Express Analysis**] to scan for viruses at this point using default settings. A new window will show the evolution of the analysis.

7.3 Watching Agent

In the Anti-virus configuration section, a scan can be configured to be performed every time a file or folder is modified. This analysis will be automatic and transparent to the User. The configuration options for this automatic analysis are the same as those described in the previous section.

Antivirus >> Watching agent



From this Antivirus configuration option, it is possible to configure the execution of machine's analysis every time that any file or folder have been modified. This kind of analysis is automatic and transparent to the user.

>> Select data source

☒ File system.
When virus found When suspicious found

Elements to analyze:

☒ Whole computer.

☒ Include CDROM/DVD drives

☒ Include USB drives

☐ Shared Folders.

☒ Include USB drives

☐ Folders or Drives.

☐ Analyze elements by file extension


OK

7.4 Updating

The Optenet Security Suite Anti-virus database can be updated automatically so that the User does not have to be concerned about keeping it up to date. If automatic database updates are not configured, Optenet Security Suite can be configured to notify the User when new updates are available for download. The User can also update the Anti-virus database manually and in real time, or schedule daily, weekly or monthly updates.

Antivirus >> Update

>> Manual update

Manual update



Update Now

>> Updating policy


☐ Don't perform programmed updates.

☒ Daily update : Hours

☐ Update weekly every at : hours

☐ Monthly at : hours


OK


7.5 Anti-virus reports

In this section, a summary report can be viewed on the scan performed by the Anti-virus. Additionally in this section, log files can be programmed to be deleted automatically to save disk space.



Antivirus >> Reports

>> Reports configuration

☒ Save reports
Report files will be deleted each days

 **Accept**



>> View reports

  **View reports**

Click on [View reports] to check Anti-virus activity log. Select the time period and the number of lines to be shown:


Antivirus >> Reports

>> Reports

 Start date: / / Start hour:
End date: / / End hour:
Number of lines to show:  **Show**

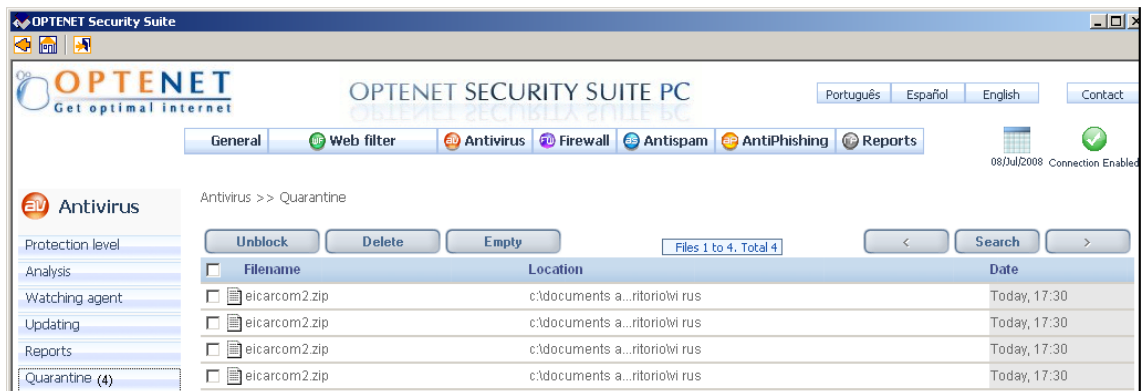
>> Reports:


26/Mar/2010:18:11:33	Analysing file system.
26/Mar/2010:18:11:35	File system analysed: 1 files analysed, 0 infected.
26/Mar/2010:18:11:35	Analysis done.
26/Mar/2010:18:30:43	Analysis started.
26/Mar/2010:18:31:13	Analysing file system.
26/Mar/2010:18:31:50	File c:\windows\driver cache\i386\driver.cab Error error: ScanFile, c:\windows\driver cache\i386\driver.cab: 7
26/Mar/2010:18:37:23	File system analysed: 9168 files analysed, 0 infected.
26/Mar/2010:18:37:24	Analysis cancelled.
26/Mar/2010:19:09:39	Analysis started.
26/Mar/2010:19:09:45	Analysing file system.
26/Mar/2010:19:09:45	File system analysed: 128 files analysed, 0 infected.
26/Mar/2010:19:09:45	Analysis cancelled.

 **Back**

7.6 Quarantine

In this section, the files in quarantine can be viewed. These files can be unblocked or deleted. The files can also be searched or the entire contents of the quarantine can be deleted (empty the quarantine).



 Note: the menu [Quarantine] (on the left), will also indicate the number of quarantined files.

8 FIREWALL

Optenet Security Suite includes a powerful Firewall that is easy to configure.

When the *[Firewall]* tab is clicked, this menu will be displayed on the left:



8.1 Security Level

In the Optenet Security Suite Firewall section, the level of security for the computer can be configured. The available levels of security are:

- High
- Recommended
- Customized

Both in *[High]* and *[Recommended]* levels, preset configuration will be used. ⚠ Only in case of selecting the *[Customized]* Protection level, changes to the configuration being done in the different sections will be allowed to be saved.

Firewall >> Security level

>> **Security level**

Customized

Security level : Customized

In the customized level you will be able to modify the configuration using the links of the horizontal menu


8.2 Application Control

In this section, access to the Internet can be granted to applications.

Initially, the list includes applications that normally have access to the Internet when they are executed.

Firewall >> Application configuration

>> **Application configuration**

 In this option you can add, modify or delete applications that have access to the Internet. By adding applications to this list, you can grant access to the Internet to those applications. Initially, the list has some applications that normally have access to the Internet when they are executed.

☒ Ask each time the application executes.
☒ Activate sound alerts.

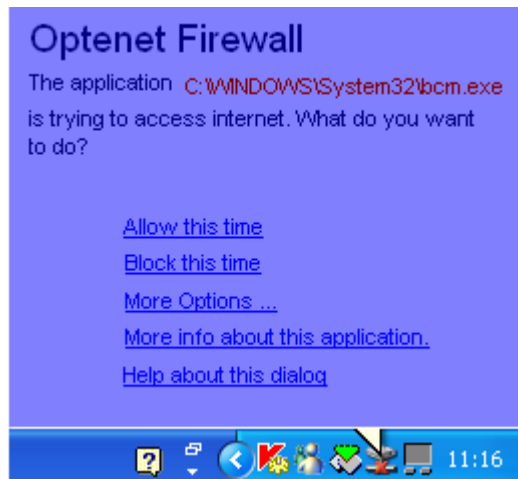
Apply the following default action: Block this time

Allow or block services (inbound/outbound) to the following applications:

Application
Predefined applications
Preset Configuration.
Operating System Applications
Other applications
C:\WINDOWS\System32\services.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\telnet.exe
C:\WINDOWS\system32\netstat.exe
C:\WINDOWS\system32\FTP.EXE

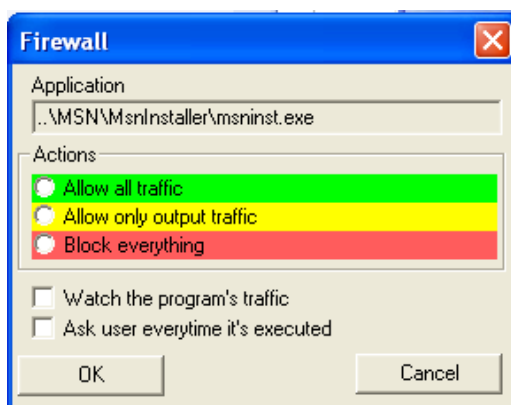
Add Delete Change

- The firewall can be configured so that it alerts the User whenever any new (unknown) application (not included in the list) attempts to access the Internet and optionally activate sound alerts.
 - » If alerts are activated, whenever an application tries to access the Internet a balloon will be shown over the Optenet Security Suite icon (on the windows status bar), asking for instructions and the appropriate action to take:



- Allow this time: This time, access to Internet will be permitted.
- Block this time: This time, access to Internet will be blocked.
- More options ...: (see next image):
- More information about this application: Obtain additional information about the application (if available).
- Help about this dialog.

If no action is chosen after a given period of time, the default action will be applied (See below).

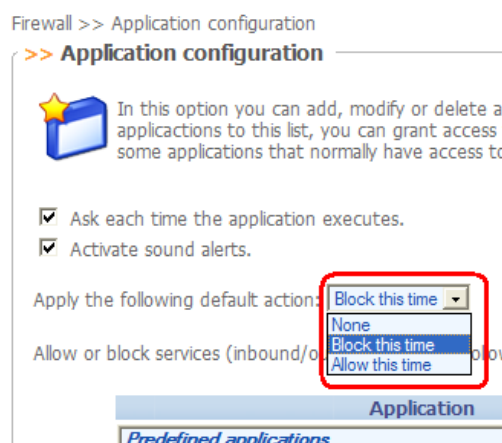


If [More options] is selected, this dialog will be shown, enabling the configuration of default options for this application to be applied whenever it tries to access Internet:

- » Enable all traffic.
 - » Enable only outbound traffic.
 - » Block all communications
- And optionally:
- » Monitor program activity
 - » Ask each time the program executes.

These options are saved to the list of known applications, and can be edited at any time.

- » Select the default action to be taken whenever any new application attempts to access Internet (or if a prompt for action to be taken has been indicated), and no option has been selected in a given period of time:



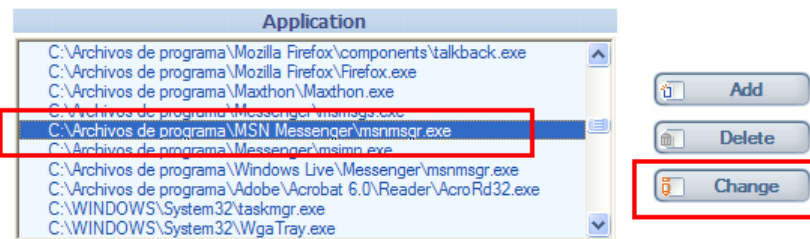
Options:

If the User does not choose what to do, default action will be:

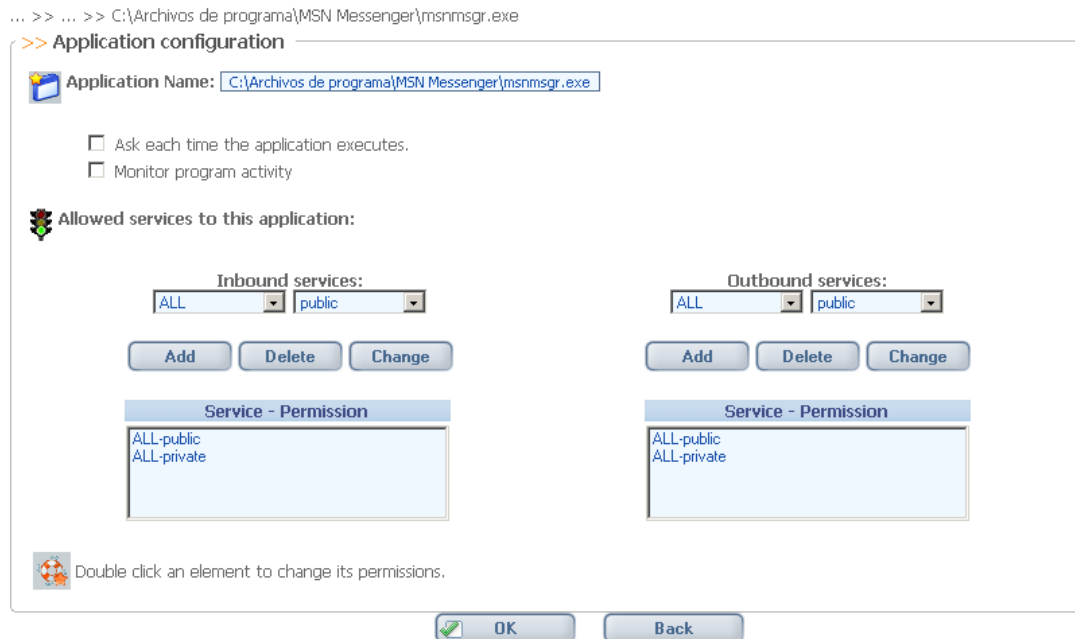
- Block this time: This time, the access to the Internet will be denied (recommended).
- Allow this time: This time, the application will have access to Internet.
- None: Keep on prompting for what to do until the User chooses an option.

For each application in the list, the types of inbound and outbound services that are allowed or denied can be configured. Select an application from the list and click on [Change]:

Allow or block services (inbound/outbound) to the following applications:



A new window will be displayed enabling specific behavior for this application to be configured:



The inbound and outbound services are:

Services:		
DHCP	DHCP	DHCP
DNS	FTP	HNS
HTTP	HTTPS	IKE
NetBios	NPP	POP3
RLP	SFTP	SMB
SMTP	SSH	TELNET
UPNP	RDP	RPC
RLP		

Additionally these services can be:

- Public
- Private.


See later in this manual how to create/customize services.

8.3 Network entries

In this section, connections established from the machine can be monitored in real-time. Only applications entered on the relevant list (Application Configuration section) are monitored. This section provides the following information about live connections:


- **Protocol:** type of communication protocol of the connection.
- **Listening IP:** IP address against which the connection has been established.
- **Listening port:** the port on which the connection has been established.
- **Application:** the application that has established the connection or listening ports (even though there is no active connection).
- **Status:** the status of the connection (private, public, blocked)

>> Network entries

 You can monitor network connections established into your PC for any application added to the applications list ("Applications" section). This option shows the following information about the current connections:

Protocol: connection communication protocol type.
Network: IP used in connection.
Port: port used in connection.
Application: application for current connection.
Status: connection status.

Protocol	Listening IP	Listening port	Application	State
TCP	192.168.142.7	139	SYSTEM	private
TCP	0.0.0.0	13590	C:\ARCHIVOS DE PROGRAMA\OPTENET SECURITY SUITE\BIN\OPT_PMON.EXE	public
TCP	0.0.0.0	135	C:\WINDOWS\SYSTEM32\SVCHOST.EXE	private
TCP	0.0.0.0	445	SYSTEM	private
TCP	0.0.0.0	10237	C:\ARCHIVOS DE PROGRAMA\OPTENET SECURITY SUITE\BIN\OPT_SECS.EXE	public
TCP	127.0.0.1	1029	C:\WINDOWS\SYSTEM32\ALG.EXE	private
UDP	192.168.142.7	137	SYSTEM	private
UDP	0.0.0.0	4500	C:\WINDOWS\SYSTEM32\LSASS.EXE	blocked
UDP	0.0.0.0	445	SYSTEM	private
UDP	0.0.0.0	500	C:\WINDOWS\SYSTEM32\LSASS.EXE	private
UDP	127.0.0.1	2659	C:\ARCHIVOS DE PROGRAMA\OPTENET SECURITY SUITE\BIN\SSBROWSER\OPT_BRWS.EXE	public
UDP	127.0.0.1	1900	C:\WINDOWS\SYSTEM32\SVCHOST.EXE	private
UDP	127.0.0.1	123	C:\WINDOWS\SYSTEM32\SVCHOST.EXE	blocked
UDP	192.168.142.7	1900	C:\WINDOWS\SYSTEM32\SVCHOST.EXE	private
UDP	192.168.142.7	123	C:\WINDOWS\SYSTEM32\SVCHOST.EXE	blocked
UDP	192.168.142.7	138	SYSTEM	private

 Refresh

8.4 IP Configuration (IP Black & White Lists)

In the Firewall configuration section, two lists of IPs can be defined:

- **Allowed IPs:** White list of IPs with which the computer can establish a connection.
- **Blocked IPs:** Black list of IPs that are unable to establish a connection with the computer.

Firewall >> IP configuration

8.5 Service Configuration

The services defined in this section will be the ones that can be used by applications (allowed, denied etc) e.g: define that telnet.exe can apply telnet services that in turn are defined as a set of TCP and/or UDP Port ranges.

Specific services can be created defining TCP and UDP port ranges to be allowed or blocked (when used by the different applications).

Firewall >> Services configuration

The services configured by default are:

Service	Description
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6 Client

Service	Description
DHCP	Dynamic Host Configuration Protocol version 6 Server
DNS	Domain Name Service
FTP	File Transfer Protocol
HNS	Host Name Server
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IKE	Internet Key Exchange
NETBIOS	Network Basic Input Output System
NPP	Network Printing Protocol
POP3	Post Office Protocol version 3
RDP	Remote Desktop Protocol
RLP	Resource Location Protocol
RPC	Remote Procedure Call
SFTP	Simple File Transfer Protocol
Telnet	Remote character terminal
SMB	Service Message Block
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
TELNET	
UPNP	Universal Plug and Play

New services can be added to this list by defining their TCP and UDP ports:

Firewall >> Services configuration >> Add

Service Name :

Service Description :

UDP ports

>> Port

>> Range

Beginning end

TCP ports

>> Port

>> Range

Beginning end

8.6 Protocols

In this section, this option regulates protocols to block, allow or allow only according to a given schedule. It is a shortcut to the Protocol Manager described before for the Web Filter Service (WebFilter >> Protocols):

P2P
Instant Messenger
Email
Newsgroup
Chat
Virtual Worlds
Others

This option regulates the use of P2P applications (Kazaa, Emule, Gnutella, etc) that allow users to share information: images, films, videos, software, etc.



>> Use of programs and applications

☒ Allowed
☐ Blocked
☐ Scheduled

>> Surf schedule

Days	Intervals					
Monday		to			to	
Tuesday		to			to	
Wednesday		to			to	
Thursday		to			to	
Friday		to			to	
Saturday		to			to	
Sunday		to			to	

Example: 08:00-09:30 12:00-14:00 19:00-22:00 (You can configure up to three periods)

 Save Configuration
 Restore Configuration

8.7 Reports


In this section, a summary report can be viewed on the actions taken by the Firewall. Additionally in this section, log files to be deleted automatically to save disk space can be programmed.

The time period can be defined for the report as well as how many lines the report should display.


Firewall >> Reports

>> Reports configuration

☒ Save reports
Report files will be deleted each days

 Accept

>> View reports

 View reports

OPTENET Security Suite

OPTENET
Get optimal Internet

OPTENET SECURITY SUITE PC

Portugu s Espa ol English Contact

General Web filter Antivirus Firewall Antispam AntiPhishing Reports


08/Jul/2008 Connection Enabled

FW Firewall

Security level
Applications
Networks
IPs
Services
Reports


Firewall >> Reports

>> Reports

Start date: 30 / Jun / 2008 Start hour: 00
End date: 07 / Jul / 2008 End hour: 23
Number of lines to show: 25 

>> Reports:

03/Jul/2008 13:30:14	[System]	LISTEN	TCP	0.0.0.0:445	-	ALLOW	[]
03/Jul/2008 13:30:14	[System]	LISTEN	TCP	192.168.142.7:139	-	ALLOW	[]
03/Jul/2008 13:30:14	[C:\WINDOWS\system32\svchost.exe]	LISTEN	TCP	0.0.0.0:135	-	ALLOW	[]
03/Jul/2008 13:30:14	[System]	OUT	UDP	192.168.142.7:137	-	DENY	[]
03/Jul/2008 13:30:14	[C:\Archivos de programa\OPTENET Security Suite\bin\OPT_SecS.exe]	LISTEN	TCP	0.0.0.0:10237	-	ALLOW	[]
03/Jul/2008 13:30:25	[C:\Archivos de programa\RealVNC\RealVNC4.exe]	LISTEN	TCP	0.0.0.0:5900	-	ALLOW	[]
03/Jul/2008 13:30:25	[C:\Archivos de programa\RealVNC\RealVNC4.exe]	LISTEN	TCP	0.0.0.0:5900	-	ALLOW	[]
03/Jul/2008 13:30:26	[I]	NOT_LISTEN	TCP	0.0.0.0:5900	-	ALLOW	[]
03/Jul/2008 13:30:26	[C:\Archivos de programa\RealVNC\RealVNC4.exe]	LISTEN	TCP	0.0.0.0:5900	-	ALLOW	[]
03/Jul/2008 13:30:30	[C:\Archivos de programa\OPTENET Security Suite\bin\OPT_FMON.exe]	LISTEN	TCP	0.0.0.0:13590	-	ALLOW	[]

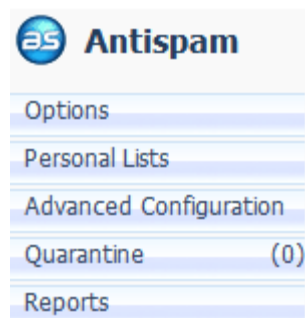
 Back

9 ANTI-SPAM

Optenet Security Suite includes a comprehensive and powerful Spam protection that helps combat the ever-increasing amount of Internet Spam.

In this section, the tool can be configured for Spam detection and access to quarantined emails.

When the [Anti-spam] tab is clicked, this menu will be displayed on the left:



9.1 Options

In this screen, the action to be taken whenever a Spam email is detected can be selected:

- Send it to Quarantine – Quarantine can be reviewed at any time, and the decision on the action to be taken regarding the email.
- Tag it – a tag will be added to Spam emails. This tag can be customized by the User and added to the following locations:
 - » Subject [Prefix] – as a prefix in the subject of the email
 - » Subject [Replace] – the tag will replace the subject of the email
 - » Body – the tag will be added at the beginning of the body of the email
 - » Send as attachment – the original email will be added as an attachment to the final email.
- Delete it – Spam emails will be deleted automatically.

Antispam >> Options

>> Actions on spam

What do you want to do with undesirable mail?

☐ Send it to Quarantine
☒ Tag it with: in
☐ Delete it

 OK

9.2 Personal Lists (Black & White Lists)

This section is for the creation of personal Black and White lists (Trusted list of Senders, Banned list of senders).

- Emails received from senders in the Trusted List will not be considered Spam by the filter.
- Emails received from senders in the Banned List will be considered as Spam and processed according to the settings chosen in the [Anti-spam>> Options] section.


Addresses to the lists on the left can be added by manually entering the address or copying a list of addresses from an external source. Existing addresses can be deleted by selecting them in the right lists and clicking [Delete].

 When copying and pasting a list of addresses please ensure that each email address is in one line.

Antispam >> Personal Lists

>> Trusted list


Senders to be accepted:




☐ Only accept emails from senders in the Trusted list

>> Banned list

Senders to be rejected:



 OK

9.3 Advanced Configuration

Advanced configuration options for Anti-spam service:

Antispam >> Advanced Configuration

The options available on this page are advanced configuration options and should not be modified unless necessary. If you are in any doubt as to whether you should change the settings below please contact our Technical Support Team.

>> Filtering categories

Select the categories you want to use for filtering. Email messages containing URL hyperlinks from the selected categories will be marked as Spam and processed according to the configuration set in the Options section.

☒ Pornography ☒ Spam advertisers

>> Filter behaviour

☒ Do not scan emails larger than KB

>> File types to block

Select the file types you do not want to receive. Email messages containing files of the type or types selected will be marked as Spam and processed according to the configuration set in the Options section.

Available file types:

Shared Files
ARJ
RAR
ZIP
Images
BMP (Microsoft Windows)
GIF
JPG (JPEG)
JPEG
PNG

Other file types:

Selected file types:

It is possible here to configure:

- **Filtering categories:** Emails including URL links to websites classified as any of the selected categories will also be considered as Spam and processed according to the settings chosen in the [Anti-spam >> Options] section. Available categories:
 - » "Pornography"
 - » "Spam advertisers"
- **Filter behaviour:** in this section, the maximum file size of emails to be analyzed (in KB) can be defined. When an email exceeds the specified size, even if it contains Spam characteristics, it will not be identified as Spam.
 - » Recommended value: 128 Kb (usually, Spam emails, even including attached files, are small).
- **File types to block:** in this section, file type(s) can be defined as undesirable not be received in the email inbox.

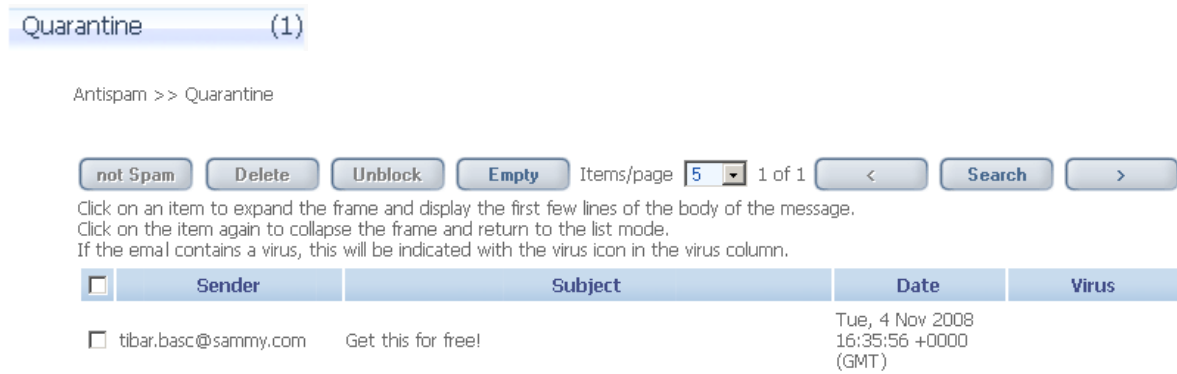
Email messages containing files of the selected file types as attachments will be considered as Spam and processed according to the settings chosen in the [Anti-spam>> Options] section.

- » Select predefined file extensions from the list or
- » Include additional file types by entering their file extension.

9.4 Quarantine

In this section, the emails sent to quarantine can be reviewed.


The number of emails in quarantine is displayed next to the menu on the left.



Choose the number of emails to be shown per page (5, 10, 25, 50, 100).

Individual emails can be selected and any of the following actions can be applied to the selected emails:

- **Not Spam:** Selected emails should not have been considered as Spam. These will be sent to User's email inbox.
- **Unblock:** Selected emails, regardless whether they are Spam or not, will be unblocked and sent to the User's email inbox.
- **Delete:** Delete selected emails (these will not be sent to User's inbox).
- **Empty:** Delete all existing emails in quarantine (even though these are not selected).

 Where a given email contains a virus, a specific icon will be displayed on the [Virus] column.

If the list of Spam Emails is too long, the list can be filtered by indicating selection criteria based on:

- » Range of dates when the email was received.
- » Sender email
- » Subject

The list of results can be placed in order (ascending or descending) by:

- » Date
- » Sender
- » Subject

Antispam >> Quarantine Search

>> Search

 Start date: 30 / Mar / 2010 20 : 00

End date: 30 / Mar / 2010 20 : 00

Sender:

Subject:

Sort by: Date ☐ Inverse order

9.4.1 Quarantine Configuration

Antispam >> Quarantine >> Configuration

>> Quarantine configuration

If a quarantined message is marked as Not Spam by user, the sender will be added to the Trusted list:

Quarantined messages will be deleted after 40 days

This screen can be accessed through a sub-menu in Quarantine and allows the following quarantine options to be configured:

- Whether the sender has to be added to the Trusted list automatically, whenever an email is checked as **Not Spam** by User. Default value: Do not add automatically to Trusted List.
- Period to maintain messages in Quarantine. Once this time has elapsed, emails will be removed automatically.

9.5 Reports

Emails that have been considered as Spam by the filter can be viewed. Reports only show information related to traffic while the filter was active.

In this section, it is possible to:

- Decide whether to save information about emails considered as Spam or not.
 - » Mark the checkbox [Save reports] to log this information.
 - » Decide the periodicity of the deletion of report files (in order to save disk space). By default this is set to 15 days.
- View Anti-spam detection history (information available where [Save reports] option has been checked).

Antispam >> Reports

>> Reports configuration

☐ Save reportsReport files will be deleted each days Accept

>> View reports

 View reports

Click on [View Reports] to define:

- Time range (from date to date)
- Number of lines to show (number of Spam emails to show):

Antispam >> Reports

>> Reports

Start date: / / Start hour: End date: / / End hour: Number of lines to show:  Show

>> Reports:

```

optenet.com 127.0.0.1 test@test.optenet.com - 04/Nov/2008:16:35:56 tibar.basc@sammy.com test@test.optenet.com 3729 Get this for
free! POP3 AC 0 - 1

```

 Back

10 ANTI-PHISHING

Optenet Security Suite includes a comprehensive and powerful Anti-phishing engine that monitors both web traffic and mail traffic, identifying suspicious activity and protecting against phishing attacks.

Optenet Anti-phishing provides:

- Protection from potential and verified fraud sites that try to obtain sensitive User information simulating other legitimate websites, including emails containing links to these sites
- Personal Data Protection: Specify credit cards, passwords, account numbers, telephone numbers, addresses or other personal key information in order to ensure that such information is used in a secure and non-fraudulent manner while browsing the Internet.

In this section, the tool can be configured for Anti-phishing detection (including access to quarantined emails) and Personal Data key definition.

When the [Anti-phishing] tab is clicked, this menu will be displayed on the left:



10.1 Options

In this screen, protection against phishing as well as the action to be taken on phishing emails or URLs can be enabled or disabled.

Antiphishing >> Options

>> **Antiphishing detection**

☒ Enable
☐ Disable

Verified phishing websites: Block / Delete
 Suspicious phishing websites: Alert / Send to quarantine

OK

There are two types of phishing websites:

- Verified Phishing sites.
- Suspicious Phishing sites

It is possible to specify different actions depending on that classification (different actions for suspicious and verified phishing sites):

- **Block/Delete:**
 - » Web: Phishing websites will be blocked (whenever navigation to those phishing URLs is attempted)
 - » Mail: Phishing emails will be automatically deleted.
- **Alert/Send to quarantine:**
 - » Web: the User will be warned that the page being accessed has been reported as a phishing website, with the action to:
 - ♦ Continue anyway.
 - ♦ Do not continue.
 - » Mail: Phishing emails will be sent to the quarantine.
- **Allow/Modify subject:**
 - » Web: access to the website will be permitted without restrictions (not recommended).
 - » Mail: Emails will be delivered but a tag will be added to the subject.

10.2 Personal Lists (Black & White Lists)

Create Black and White lists:

White List	Black List
Trusted List of Senders (email)	Banned List of Senders (email)
Trusted List of URLs	Banned List of URLs

- Trusted list of Senders: Email Senders that will never be considered as phishing sources.

- Banned list of Senders: Email Senders that will always be considered as phishing sources.
- Trusted list of URLs: URLs to be considered as not being phishing sites.
- Banned list of URLs: URLs to be considered as phishing sites.

Filter behavior:


- URLs in the Trusted list and Emails received from Trusted senders will never be considered as phishing.
- URLs in the Banned List and Emails received from Banned Senders will always be considered as phishing and processed according to the settings chosen in the [Anti-phishing>> Options] section.

Addresses to the lists on the left can be added by manually entering the address or copying a list of addresses from an external source. Existing addresses can be deleted by selecting them in the right lists and clicking [Delete].


⚠ When copying and pasting a list of addresses, ensure that each email address is in one line.

AntiPhishing >> Personal lists

>> Trusted list


 Senders to never consider phishing:

Add << Delete


 URLs to never consider phishing:

Add << Delete

>> Banned list

 Senders to always consider phishing:

Add << Delete

 URLs to always consider phishing:

Add << Delete

OK

10.3 Personal Data Protection

Personal data protection allows personal data such as credit cards, passwords, account numbers, telephone numbers, addresses or other personal key information to be entered, modified and deleted in order to ensure that such information is used in a secure and non-fraudulent manner while browsing the Internet.

In this screen, the personal data protection functionality as well as the action to be taken when the program detects an attempt to send stored personal data in the computer can be enabled or disabled:

- **Mask:** when a User enters any of the stored personal data on a website, the data will be sent encrypted in a form that cannot be recognised by the receiver (replaced by asterisks).
- **Alert:** when a User enters any of the stored personal data on a website, a message will warn him/her of the attempt to send this personal information, requesting the administrator's password.
 - » If the password is correct, the data will be sent as normal.
 - » Otherwise (or if the Cancel button is pressed) the information is sent encrypted in a form that cannot be recognised by the receiver (replaced by asterisks).

Additionally, an email account can be configured to receive notifications each time any kind of personal data is being sent (or has been attempted to be sent) to the Internet.

>> Personal Data Protection

☒ Enable Action
☐ Disable Mask

☒ Notify: myAccount@MyDomain.com

Adding Personal Data:

To configure personal data, for each section enter a name (or alias) and the value (at least four characters) for the credit card, password, telephone number, address and personal key information, and click on [Add]. The entered name appears in the List on the right.

In order to improve the security:

- Personal data will be requested to be re-entered.
- Personal data will always be displayed protected (replaced by asterisk).

Deleting Personal Data:

To delete personal data, select the element to be deleted in the list on the right, and click on [Delete].

Updating Personal Data:

To modify a value, select it in the List on the right and click on [Edit].

The relevant values will appear in the fields on the left, where they can be edited. Where a change is applied to a name (or alias), a new record will be added.


Click on [OK] to save the settings.

AntiPhishing >> Personal Data Protection


>> Personal Data Protection

☒ Enable Action
☐ Disable **Mask** ☐ Notify:

>> Credit Cards


 Card name: **Add >>**
 Card number: - - - **Delete**
 Re-enter card number: - - - **<< Edit**


>> Passwords


 Password alias: **Add >>**
 Password: **Delete**
 Re-enter password: **<< Edit**


>> Telephone Numbers



 Telephone alias: **Add >>**
 Telephone number: **Delete**
 Re-enter telephone number: **<< Edit**

>> Addresses


 Address alias: **Add >>**
 Address: **Delete**
 Re-enter address: **<< Edit**

>> Other Keys


 Key name: **Add >>**
 Key value: **Delete**
 Re-enter key value: **<< Edit**



10.4 Quarantine

In this section, emails sent to Anti-phishing quarantine can be reviewed.

The number of emails in quarantine is displayed next to the menu on the left.

Quarantine (1)

Anti-Phishing >> Quarantine

Items/page 1 of 1

Click on an item to expand the frame and display the first few lines of the body of the message.
 Click on the item again to collapse the frame and return to the list mode.
 If the email contains a virus, this will be indicated with the virus icon in the virus column.

<input type="checkbox"/>	Sender	Subject	Date	Virus
<input type="checkbox"/>	tibar.basc@sammy.com	Get this for free!	Tue, 4 Nov 2008 16:35:56 +0000 (GMT)	

Choose the number of emails to be shown per page (5, 10, 25, 50, 100).

Individual emails can be selected and any of the following actions can be applied to the selected emails:

- **Not Phishing:** Selected emails should not have been considered as Phishing. These will be sent to User's email inbox.
- **Unblock:** Selected emails, regardless whether they are phishing or not, will be unblocked and sent to the User's inbox.
- **Delete:** Delete selected emails (these will not be sent to User's inbox).
- **Empty:** Delete all existing emails in quarantine (even though these are not selected).

 Where a given email also contains a virus, a specific icon will be displayed on the [Virus] column.

AntiPhishing >> Quarantine

Items/page of

Click on an item to expand the frame and display the first few lines of the body of the message.
Click on the item again to collapse the frame and return to the list mode.
If the email contains a virus, this will be indicated with the virus icon in the virus column.

<input type="checkbox"/>	Sender	Subject	Date	Virus
<input type="checkbox"/>	tibar.basc@sammy.com	[MMAS6]Need affordable Drugs? Purchase Online here:- GenericCialis \$2.80, GenericViagra \$2.23 ytlpg rczo	Tue, 4 Nov 2008 15:26:54 +0000 (GMT)	

If the list of Phishing Emails is too long, the list can be filtered by indicating selection criteria based on:

- » Range of dates when the email was received.
- » Sender email
- » Subject

The list of results can be placed in order (ascending or descending) by:

- » Date
- » Sender
- » Subject

>> Search


 Start date: / / :
 End date: / / :
 Sender:
 Subject:
 Sort by: ☐ Inverse order

10.4.1 Quarantine Configuration

Antiphishing >> Quarantine >> Configuration

>> Quarantine configuration

If a quarantined message is marked as Not Phishing by user, the sender will be added to the Trusted list:

Quarantined messages will be deleted after days



This screen can be accessed through a sub-menu in Quarantine and allows the following quarantine options to be configured:

- Whether the sender has to be added to the Trusted list automatically, whenever an email is marked as **Not Phishing** by User. Default value: Do not add automatically to Trusted List.
- Period to maintain messages in Quarantine. Once this time has elapsed, emails will be removed automatically.

10.5 Reports

Emails that have been considered as Phishing by the filter as well as URLs that have been categorized as phishing sites can be viewed. Reports only show information related to traffic while the filter was active.

In this section, it is possible to:

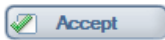
- Decide whether to save information about emails/URLs considered as phishing attacks.
 - » Mark the checkbox [Save reports] to log this information.
 - » Decide the frequency of the deletion of report files (in order to save disk space). By default this is set to 15 days.
- View Phishing detection history (information available where [Save reports] option has been checked).

Antiphishing >> Reports



>> Reports configuration

☒ Save reports

Report files will be deleted each days



>> View reports


Click on [View Reports] to define:

- Time range (from date to date)

- Number of lines to show (number of phishing attacks to show):

AntiPhishing >> Reports

>> Reports

Start date: 04 / Nov / 2008 Start hour: 00
End date: 04 / Nov / 2008 End hour: 23
Number of lines to show: 10 


>> Reports:

Antiphishing Web
NoData

Antiphishing Mail

optenet.com	127.0.0.1	test@test.optenet.com	-	04/Nov/2008:15:26:54	tibar.basci@sammy.com	test@test.optenet.com	4578	[MMAS6]Need
affordable Drugs? Purchase Online here:- GenericCialis \$2.80, GenericViagra \$2.23 ytlpg rczo POP3 AC-PHI 0 - 1								

Other
NoData



11 REPORTS

In this section, a summary of the actions taken by Optenet Security Suite can be viewed.

>> Reports

>> Reports

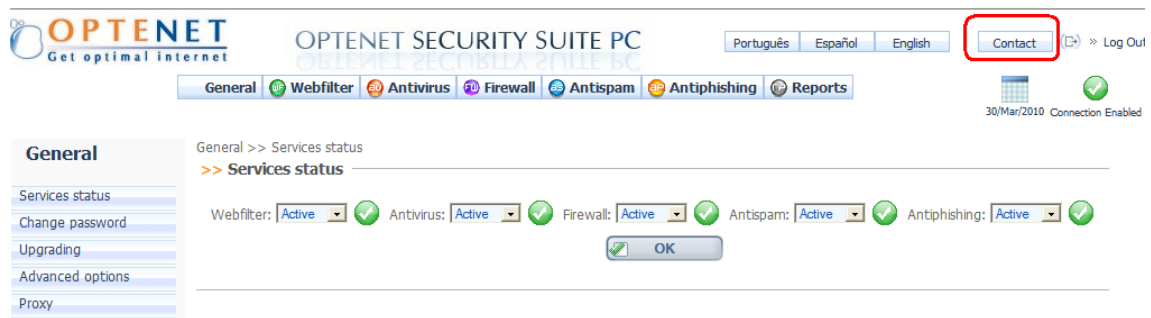


Click to view filter reports : [here](#)
Click to show antivirus reports : [here](#)
Click to view firewall reports : [here](#)
Click to view antispam reports : [here](#)
Click to view antiphishing reports : [here](#)

Reports can be viewed on the activity of the following services (list of services may vary depending on installed product):

- Web Filter
- Anti-virus
- Firewall.
- Anti-spam
- Anti-phishing

12 CONTACT SUPPORT




Click on [Contact]. A new window will be opened with the email account for:


- Customer support requests.
- Technical support requests.



13 UN-INSTALL

To un-install Optenet Security Suite, simply use the shortcut created on the computer's Start menu. During the un-installation process, the administrator password will be requested, preventing any other User from removing the program.

 **IMPORTANT:** Do not attempt to un-install the program by deleting the Security Suite directories and files since this could result in irreparable damage to the installation, causing loss of Internet access completely. Always use the shortcut on the computer to un-install the software.

 If the Optenet Security Suite installation application executes on a machine where the software is already installed, the un-installation process for the existing version will be initiated (once the administrator password has been entered) overwriting files.