

EnoLogic NetFilter Home User's Guide

Contents

1. Introduction
2. Installation
 - 2.1 System Requirements
 - 2.2 Installation of EnoLogic NetFilter
 - 2.3 Configuration of Browsers
3. Configuration & Supervision of EnoLogic NetFilter
 - 3.1 Login
 - 3.2 Navigation in EnoLogic NetFilter Admin
 - 3.3 The Filter Topic
 - 3.4 The Proxy Topic
 - 3.5. The Privacy Topic
 - 3.6 The Advanced Topic
4. Automatic updates with EnoLogic NetUpdate
5. Uninstallation
6. Troubleshooting
7. Customer Service



1. Introduction

The Internet is a wonderful place for the children to search for information and educate themselves. However, the Internet is the world's largest distribution channel for pornography and children are in high danger of being exposed to it. Many children will be confronted with hardcore pornography even if they do not themselves actively look for it. Innocent search queries may lead your child to sex sites against their will, because popular search strings like "Britney Spears" are used to lure people into these sites.

EnoLogic NetFilter Home protects your child against inappropriate content on the Internet within the following categories:

- Pornography
- Hate, racism and discrimination
- Violence and vulgar humour
- Illegal or dangerous activities
- Copyright violations (piracy)

The core of EnoLogic NetFilter is an advanced content filtering algorithm, which analyses images and text on each page that is visited. If a page is deemed inappropriate, a page with a warning that the content may be inappropriate is shown instead. You can specify whether your children can continue to such pages, or if they only are permitted to return to the previous page. If it is chosen to continue to the page in spite of the warning, it is registered in a log file.

EnoLogic NetFilter can also block chat and peer-2-peer file sharing programs, prevent disclosure of personal information, block streaming audio and video, block or log retrieval of MP3 files and large files, for instance movies and software. Additionally, it is possible to block download of files based on their name/extension.

2. Installation

The installation of EnoLogic NetFilter consists of two steps. First, EnoLogic NetFilter must be installed on the computer. Then, the web browsers on the computer must be configured to use EnoLogic NetFilter as proxy server.

2.1 System Requirements

Minimum requirements:

- 200 MHz Pentium-compatible CPU
- 32 MB RAM
- 50 MB of free space on the hard disk
- Microsoft Windows 98, ME, NT 4, 2000, or XP

All browsers that can use a HTTP proxy are, in principle, supported. The following browsers are configured automatically:

- Microsoft Internet Explorer 4 and later
- Netscape Navigator and Communicator 4
- Netscape 6 and 7 and Mozilla
- Opera 5 and 6

Other browsers may be configured manually to use EnoLogic NetFilter.

2.2 Installation of EnoLogic NetFilter

If you have an EnoLogic NetFilter installation CD-ROM, the installation will start automatically when the CD is placed in the CD-ROM drive if Windows is configured for this. If the installation does not start automatically, click *This Computer* on the Windows desktop (or Start menu in Windows XP) and double click the EnoLogic NetFilter icon. If you have downloaded the setup file from EnoLogic's web site, you must double-click on the file to start the installation.

The installation program will lead you through the steps necessary for the installation of EnoLogic NetFilter. After the installation has been completed, EnoLogic NetFilter is installed as a service and will be started automatically next time the machine is rebooted. You will be offered the choice between restarting the machine immediately or waiting.

2.3 Configuration of Browsers

The supported browsers, listed in section 2.1, are configured automatically for filtering using EnoLogic NetFilter. If you want to use filtering in another browser, this can be done by configuring it to use EnoLogic NetFilter as HTTP proxy. How this is done is typically described in the manual or help-function for the browser. The address of the NetFilter proxy is *localhost*. The port is 3128.

3. Configuration and Supervision of EnoLogic NetFilter

When the computer has been rebooted after the installation of EnoLogic NetFilter, a new icon will be shown in the status area of the taskbar (the "tray"). This tray icon shows the state of the filter and warns about potential problems.



The filter is active.



The filter is not active.



The filter is active, but one or more browsers may not be configured to use it. If a browser is not configured to use the filter, it will typically have unfiltered access to the Internet, even though the filter is active. In some cases, it will not have access to the Internet.



The filter is not active and the browsers may not be configured to use it. This can in some cases mean that the browsers do not have access to the Internet.



Status is unknown or the service EnoLogic NetFilter is not running. This will often be the case when the computer is being started. Under normal circumstances, the red cross will disappear after a few seconds.

When clicking on the tray icon with the right mouse button, a menu with the following entries is shown:

- *NetUpdate*, if EnoLogic NetUpdate is installed

- *Settings for EnoLogic NetFilter*
- *Deactivate filter* or *Activate filter*, depending on the current status of the filter
- *Status*

If *Status* is chosen, a window with status information is shown. *Deactivate filter* and *Activate filter* may be used to quickly deactivate and activate the filter and require password, as shown in Figure 1. If *Settings for EnoLogic NetFilter* is selected, the program EnoLogic NetFilter Admin is started. This program also requires password. If username and password have not been changed with EnoLogic NetFilter Admin, both are "admin".

If *NetUpdate* is chosen, the program EnoLogic NetUpdate, which is used for performing automatic updates of the installed EnoLogic products via the Internet, is started. This program is described in detail in section 4.



Figure 1: Deactivating filter from the tray icon.

The computer that EnoLogic NetFilter is running on is referred to as the filtering server. When EnoLogic NetFilter Home is installed on your computer, your computer is the filtering server. With EnoLogic NetFilter Admin, it is also possible to perform remote administration of a filtering server, if the program has been configured to show the advanced settings, as described in section 3.6.1.

The default setting for the program is not to show the advanced settings, as most private users do not need to change them, but, in the description that follows, the user interface is described as it will look if these settings are shown.

3.1 Login

When EnoLogic NetFilter Admin is started, a login window as shown in Figure 2 will appear. In this window, the IP address of the filtering server must be specified together with the number of the administration port for EnoLogic NetFilter.

Note: If EnoLogic NetFilter Admin is configured not to show the advanced settings, address and port of the filtering server cannot be specified. EnoLogic NetFilter is in this case assumed to be running on the same computer as the administration program.

If EnoLogic NetFilter Admin has been started on the filtering server, the IP address 127.0.0.1 which refers to *localhost*, that is, the computer that EnoLogic NetFilter Admin has been started on, can be left unchanged. Otherwise, the IP address of the filtering server to administrate is entered. The port number 9600 can be left unchanged, unless EnoLogic NetFilter has been manually configured to use another port. If that is the case, this port number should be entered instead. How to change the administration port is described in section 3.4.1.



Figure 2: Filtering Server Login.

For security reasons, it is necessary to login at the filtering server with username and password before it is possible to administrate it. If it is the first time EnoLogic NetFilter Admin is started, both the username and the password is "admin". It is very important that the password is changed immediately after the first login to avoid unauthorized access to

the filtering server. See section 3.6.1 for more information.

When the username and password has been entered, the *Login* button is pressed. If the login at the filtering server is successful, a screen as shown in Figure 3 will appear. If the login is not successful, an error message is shown instead.

3.2 Navigation in EnoLogic NetFilter Admin

After a successful login, a start page as shown in Figure 3 is shown. Here, the general information about version and statistics is shown. By choosing between the four topics in the upper right part of the window it is possible to navigate in EnoLogic NetFilter Admin. The topic which is activated after login is *Filter*. Some of the topics are divided into sub-topics. These are chosen by clicking on the tabs which are seen at the bottom of the window. For the *Filter* topic, the first tab is *Status*.

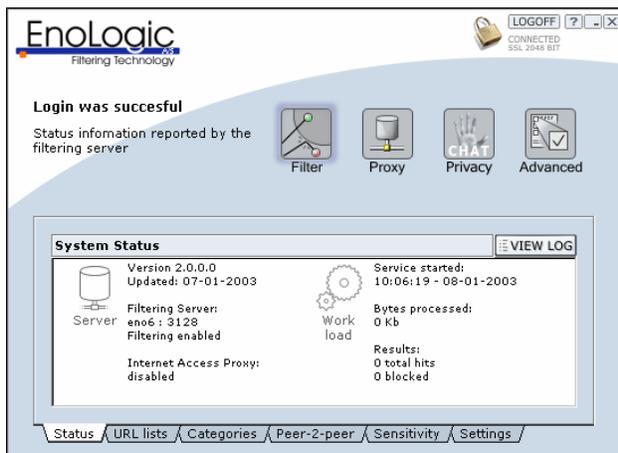


Figure 3: Status-page which is shown after login.

3.3 The Filter Topic

The *Filter* topic contains information and standard configuration options for EnoLogic NetFilter. The different tabs for *Filter* are described in the following sections.

3.3.1 Status

The tab *Status* makes it possible to see information regarding EnoLogic NetFilter. As it can be seen in Figure 3, it is possible to read the version number for

EnoLogic NetFilter, which machine and port, the filter is running on, whether filtering is activated and whether the filter is using an Internet proxy. It is also possible to see statistics regarding the filter, such as when the filter was started, how much data that have been sent through the filter measured in bytes, and how many pages that have been visited through the filter, and how many pages that were blocked.

It is also possible to be presented to at detailed statistics by pressing the button *SHOW LOG*. This will open a browser with a statistics page showing granted and blocked traffic through the filter as well as blocked attempts to disclose personal information.

3.3.2 URL-lists

3.3.2.1 Always Grant List

The tab *Always grant list*, which can be seen in Figure 4, makes it possible to add URLs that should never be blocked by EnoLogic NetFilter, no matter their content. To add an URL, it is entered in the URL field, and the button *ADD URL* is pressed. To remove an URL, it is selected with the mouse and the button *DEL URL* is pressed.

An URL in the grant list covers all sub-URLs. For instance, access to <http://www.enologic.com/test/> will always be granted with the settings shown in Figure 4. Inversely, <http://www.test.com> could be blocked even though <http://www.test.com/dirty/> has been added to the list.

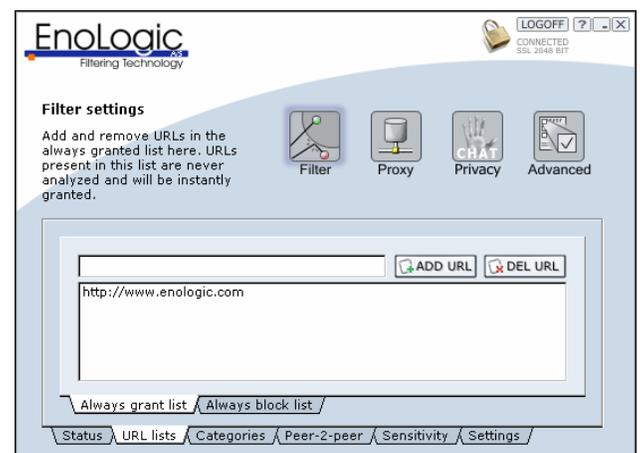


Figure 4: Always grant list. The addresses in this list will never be blocked.

3.3.2.2 Always Block List

The tab *Always block list*, shown in Figure 5, makes it possible to add URLs that no matter their content must be blocked. This makes it possible to add pages that are not included in the categories, for instance, gambling or other unwanted material. To add an URL, it is entered in the URL field and the button *ADD URL* is pressed. To remove a URL, select it with the mouse and press *DEL URL*.

An URL which is specified in the block list covers all sub-URLs.

For instance, <http://www.gambling.com/test/> will always be blocked with the settings shown in Figure 5. Inversely, <http://www.test.com> may be granted even though <http://www.test.com/dirty/> has been added to the list.

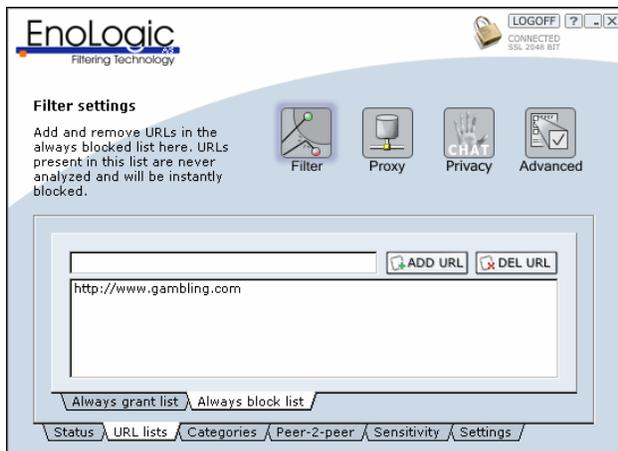


Figure 5: *Always block list.* The addresses in this list will always be blocked.

3.3.3 Categories

Under *Categories*, it is possible to choose which categories the filter must block. This is done by checking the desired categories in the list shown in Figure 6. When a category is marked, a description of the category is shown to the right.

The following categories are supported:

- *Pornography.* Pages with pornographic content. Sexually educative pages are only

blocked if the content is very explicit or extreme.

- *Hate, racism and discrimination.* Pages that based on race, religion, or sexual orientation advocate discrimination against a group, express hate toward a group, encourage attacks on a group, or present one group as being superior to others.
- *Violence and vulgar humour.* Pages with violent or gross content related to violence, murder, suicide, death, accidents, disease, body modifications, cannibalism, necrophilia, and bodily functions.
- *Copyright violations.* Pages that violates copyright by offering or providing access to software, movies, music, etc.
- *Illegal or dangerous activities.* Pages that provides instructions for construction/production of and illegal or dangerous use of weapons, explosives, fireworks, and toxic chemicals, credit card fraud, burglary and theft, and other criminal or dangerous activities.

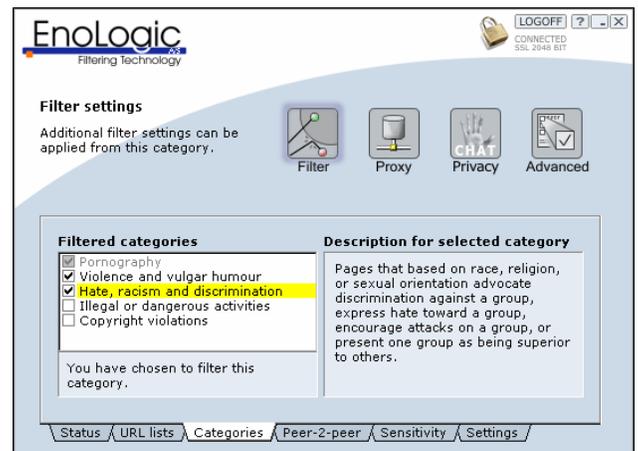


Figure 6: *Categories.* The filter blocks the categories that have been selected in the list.

3.3.4 Peer-2-peer

The tab *Peer-2-peer* makes it possible to block peer-2-peer programs that are used for distribution of software, music, movies, etc. between computers on

the Internet. The two most important reasons for blocking these programs are, that the files, that are exchanged often are large and therefore expensive to transfer, and that the programs often are used for piracy.

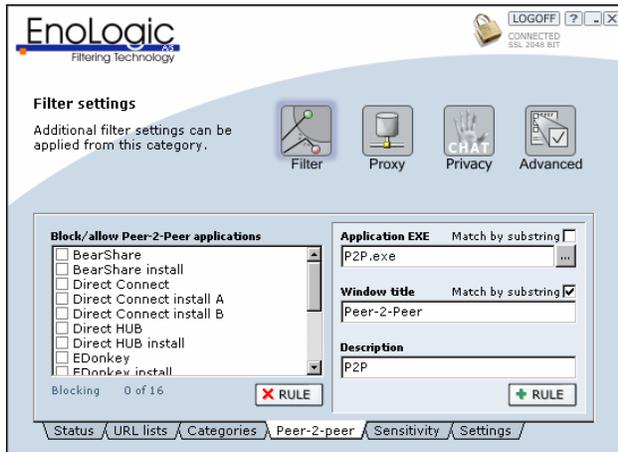


Figure 7: Blocking of peer-2-peer programs.

In the list to the left in Figure 7, it can be chosen which peer-2-peer programs that must be blocked. The built-in list contains the most common peer-2-peer programs and you may add more programs yourself.

If you right-click on the list, a menu with the following functions is displayed:

- *Block all defaults.* This activates blocking of the programs in the built-in list.
- *Allow all defaults.* This deactivates blocking of the programs in the built-in list.
- *Block all.* This activates blocking of all programs in the list, including those added by the user.
- *Allow all.* This deactivates blocking of all programs in the list, including those added by the user.

To add a program to the list, the name of the EXE-file of the program and/or the title of its window is entered. In the field *Description*, the name that you want to appear in the list is entered. The program is added by pressing *+RULE*.

When the button with the three dots to the right of the text field for the filename is pressed, a window is opened, where the file may be selected.

If both filename and window title are entered, programs with either the specified filename or window title are blocked.

It is possible to match by substring for both filename and window title. In the case of the filename, this means that the program is blocked if the name of its EXE-file contains the specified text. For instance, if you specify "p2p" as filename and checks *Match by substring*, "p2p.exe", "myp2p.exe" and "p2p program.exe" will be blocked. Substring matching works in the same way for the window title. Substring matching should be used with care, as you otherwise risk blocking a wrong program.

The blocking works by closing the programs. Some seconds may pass before this happens. If the window title is used for matching, the program is only closed if the window is active.

A program that has been added by the user may be removed from the list by selecting it and pressing *XRULE*. The programs in the built-in list cannot be removed.

3.3.4 Sensitivity

As shown in Figure 8, the tab *Sensitivity* makes it possible to adjust the sensitivity of EnoLogic NetFilter with regard to inappropriate material. It is possible to choose between three settings for sensitivity, *Low*, *Normal*, and *High*.

If *Low* sensitivity is chosen, the filter will perform a less aggressive analysis, which implies that more pages will be granted as being appropriate by the filter. This setting can be ideal, if you wish a less restrictive filter. The risk that inappropriate material will get through the filter is greater when the sensitivity is set to *Low*, but the risk that material that is not inappropriate will be blocked is lower.

Normal is the standard setting for the filter and is recommended for normal use.

High sensitivity can be chosen if a more aggressive analysis is wanted. This means that the filter is more sensitive to inappropriate material. This setting will

cause more pages to be considered inappropriate. The risk that the filter will classify appropriate pages as inappropriate is greater, but the risk that inappropriate material gets through the filter is lower.

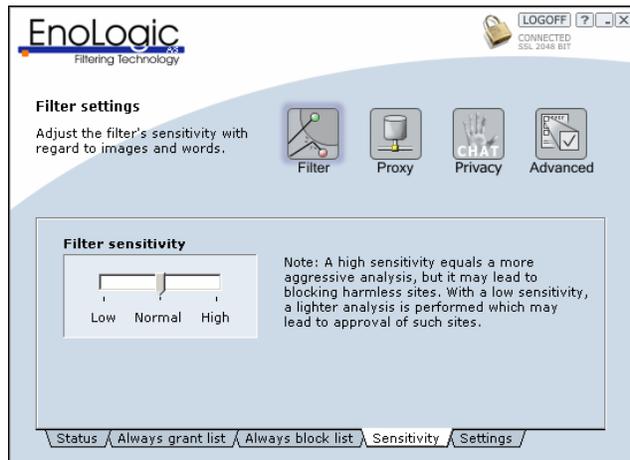


Figure 8: Adjustment of the sensitivity of the filter.

3.3.5 Settings

The tab *Settings* makes it possible to activate and deactivate various properties of the filter. The page is divided into a series of tabs for the different properties.

Under the tab *General*, shown in Figure 9, the following options are available:

- *Disable filter completely*. Makes it possible to turn filtering on and off. Can be useful if you for a short period wish to allow all traffic on your network.
- *Optimized modem mode*. When this is checked, the filter is optimized for slow Internet connections such as 56 Kbps modem. If you use modem or another slow connection, it is recommended that you activate this.

Under the tab *MP3 analysis*, shown in Figure 10, detection and blocking of MP3 files may be configured:

- *Enable MP3 detection*. If this property is enabled, all MP3 traffic will be registered in

the log file. MP3 detection requires a little more resources when enabled. Detection and blocking of MP3 is based on content analysis. That is, the filter also detects MP3 files even if they are "disguised" as other files. For instance, the file MichaelJackson.gif will be detected/blocked if it is a renamed MP3 file.

- *Block all MP3 data*. Blocks MP3 traffic. As MP3 detection, this property will also cause a slightly larger demand for resources.

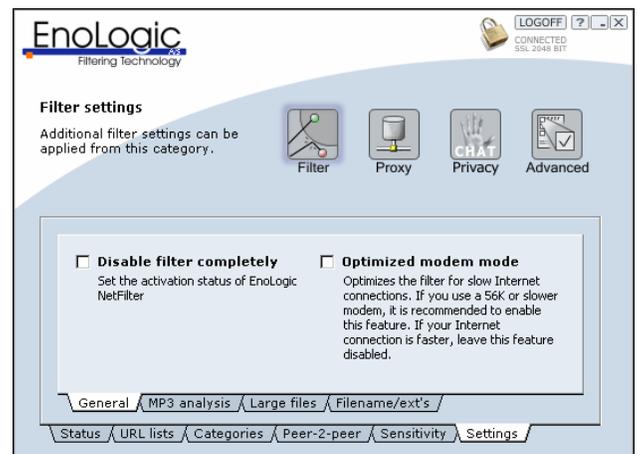


Figure 9: General settings for the filter.

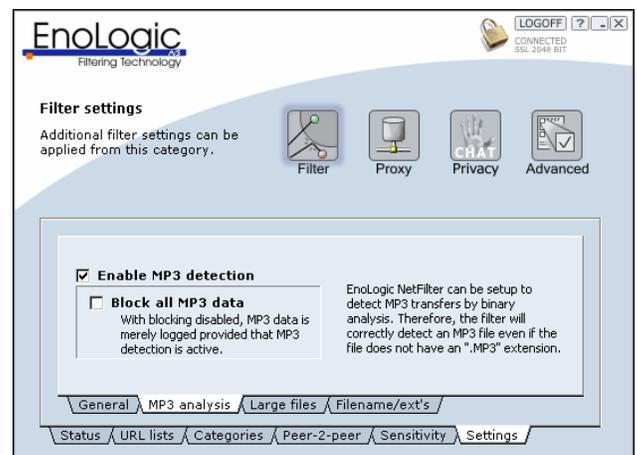


Figure 10: MP3 detections and blocking.

Under the tab *Large files*, shown in Figure 11, detection and blocking of large files may be configured:

- *Enable large file detection.* It is possible to detect large files passing through the filter. This property makes it possible to determine whether traffic of such files occurs. If this is the case, it will be written to the log file. Depending on the circumstances, it may be different when a file is considered large. Therefore, it is possible to specify how large a file must be for it to be considered large. According to the standard setting, a file is large if it is larger than 5.000.000 bytes (approx. 5 MB).
- *Block files larger than.* Block for transfer of files larger than the specified limit and register transfer attempts in the log file.

Under the tab *Filename/ext's*, shown in Figure 12, it is possible to configure blocking using rules based on the filename.

If *Block common streaming media types* is checked, rules for the most common types of streaming media are added.

It is possible to add rules in three different categories:

- *Only extension.* Enter extension, for instance "exe" or "zip", in the text field and press *+RULE* to add the extension to the list. Now, all files with the specified extension will be blocked.
- *Exact filename.* To block files with a specific name, enter the filename, e.g. "foo.exe", in the text field. Then press *+RULE* to add it to the list.
- *Substring in filename.* Use this category to block a file which has a name that contains a particular text. Enter the text that the file name must contain in the text field and press *+RULE* to add the rule.

A rule may be deleted by selecting the rule in the list and pressing *XRULE*.

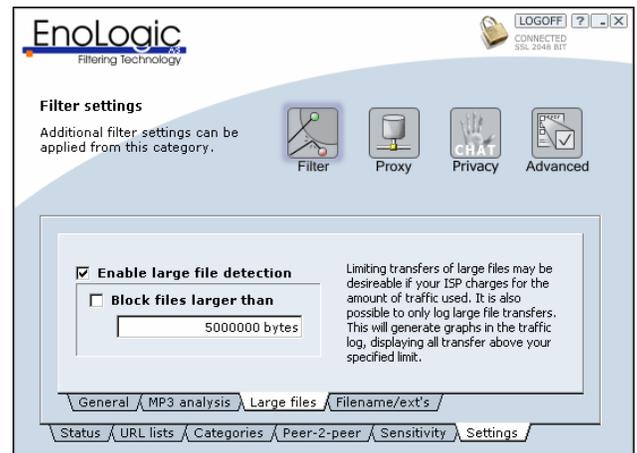


Figure 11: Large file detection and blocking.

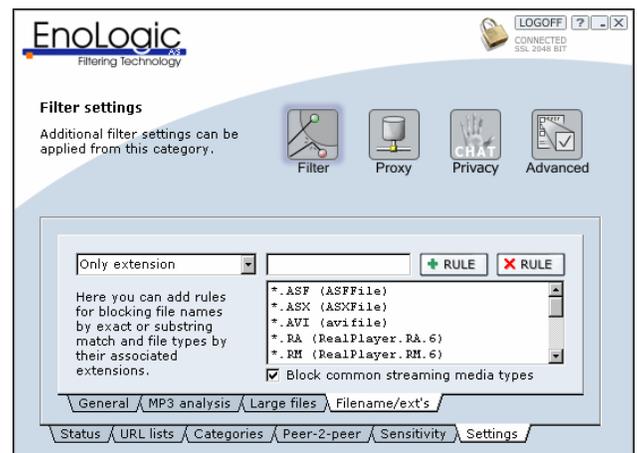


Figure 12: Blocking by name.

3.4 The Proxy Topic

This topic makes it possible to configure which ports EnoLogic NetFilter operates on, as well as whether the traffic from EnoLogic NetFilter should be directed through an external proxy. A screenshot from the Proxy topic is shown in Figure 13.

3.4.1 NetFilter Proxy

Here, it is possible to configure which port that is to be used by browsers for Internet access through EnoLogic NetFilter. The default value for this port is 3128, which is the port usually used for proxy servers. If another port is desired, it is entered in the *Filter Port* field. If EnoLogic NetFilter is used without an external proxy server, it is usually not necessary

to change this port. See below for more information about use of an external proxy server.

It is also possible to change the port on EnoLogic NetFilter that is used for communication with EnoLogic NetFilter Admin. This is originally set to 9600. If another port is wanted, it is entered in the *Admin Port* field. Remember, that by subsequent logins from EnoLogic NetFilter Admin, the new port must be entered instead, as described in section 3.1.

The modifications of the port settings will not be activated until the *APPLY* button has been pressed. Please note, that EnoLogic NetFilter for a short period of time will be inactive while it adapts to the changes.

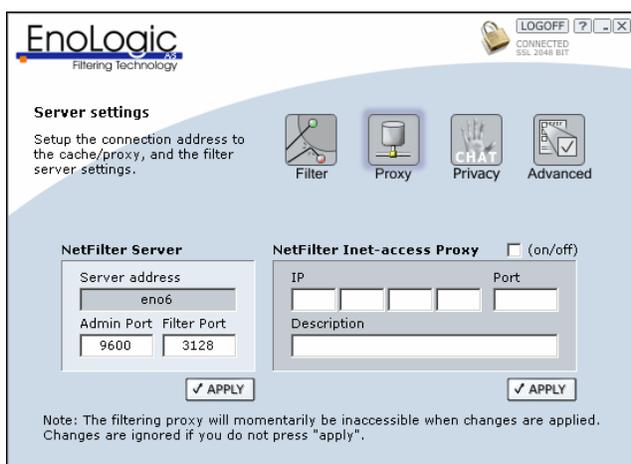


Figure 13: Configuration of EnoLogic NetFilter port numbers and external proxy.

3.4.2 NetFilter Inet-access Proxy

It is possible to connect EnoLogic NetFilter with an external proxy server. This can be an advantage if, for instance, a proxy server is already in use on the network. The Internet access will happen through the external proxy server, and EnoLogic NetFilter will filter the traffic between the external proxy and the clients.

To direct the traffic through an external proxy server, the IP address of the external proxy server is entered in the field *IP* under *NetFilter Inet-access Proxy*. Likewise, the port of the external proxy server is specified in the field *Port*. Furthermore, it is possible to add a description of the external proxy server. This

information is not used by EnoLogic NetFilter, but is solely for your own use (e.g. the DNS name of the proxy).

Any changes are activated by clicking the *APPLY* button, provided that the field *on/off* is checked. Note that EnoLogic NetFilter for a short period will be inactive while it adapts to the changes.

3.5. The Privacy Topic

Under *Privacy*, it is possible activate filtering or blocking of chat.

3.5.1 Chat blocking

The page for chat blocking is shown in Figure 14. In the list to the left, it is possible to choose which types of chat that must be blocked. If *Browser/web chat* is checked, web sites that offer chat will be blocked. The other entries in the list are some of the most common chat programs.

If you right-click on the list, a menu with the following functions is displayed:

- *Block all defaults.* This activates blocking of the programs in the built-in list.
- *Allow all defaults.* This deactivates blocking of the programs in the built-in list.
- *Block all.* This activates blocking of all programs in the list, including those added by the user.
- *Allow all.* This deactivates blocking of all programs in the list, including those added by the user.

To add a program to the list, the name of the EXE-file of the program and/or the title of its window is entered. In the field *Description*, the name that you want to appear in the list is entered. The program is added by pressing *+RULE*.

When the button with the three dots to the right of the text field for the filename is pressed, a window is opened, where the file may be selected.

If both filename and window title are entered, programs with either the specified filename or window title are blocked.

It is possible to match by substring for both filename and window title. In the case of the filename, this means that the program is blocked if the name of its EXE-file contains the specified text. For instance, if you specify "chat" as filename and checks *Match by substring*, "chat.exe", "mychat.exe" and "chat program.exe" will be blocked. Substring matching works in the same way for the window title. Substring matching should be used with care, as you otherwise risk blocking a wrong program.

The blocking works by closing the programs. Some seconds may pass before this happens. If the window title is used for matching, the program is only closed if the window is active.

A program that has been added by the user may be removed from the list by selecting it and pressing *XRULE*. The programs in the built-in list cannot be removed.

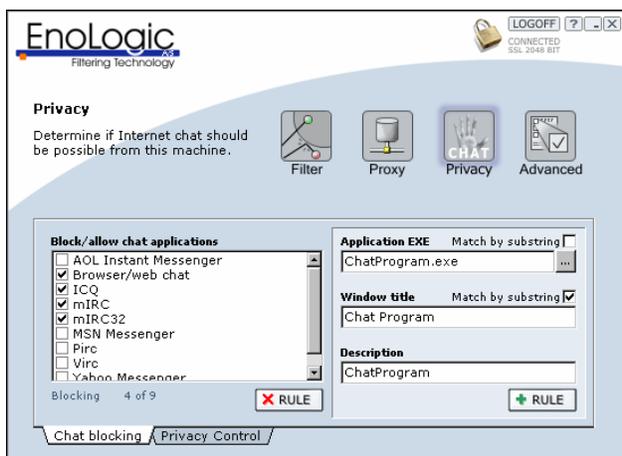


Figure 14: Chat blocking.

3.5.2 Privacy Control

On the page *Personal information* it is, as shown in Figure 15, possible to specify information that should remain private. By entering such information here, it is prevented that it is disclosed to strangers via the Internet.

The information may include surname, address, and telephone number. If you have children who use the Internet for chat, it is recommended that this function is used to protect them against pedophiles and others who try to lure them into providing this

information with the purpose of subsequently contacting them.

To activate this function, the field *Block transmission of confidential data* must be checked. Then, information may be added by choosing the type of information under *Type* and entering a text in the field under *Confidential data*. When *Add* is pressed, the entered will be added to the list. To remove a previously added piece of information, it is chosen from the list, and *Remove* is pressed.

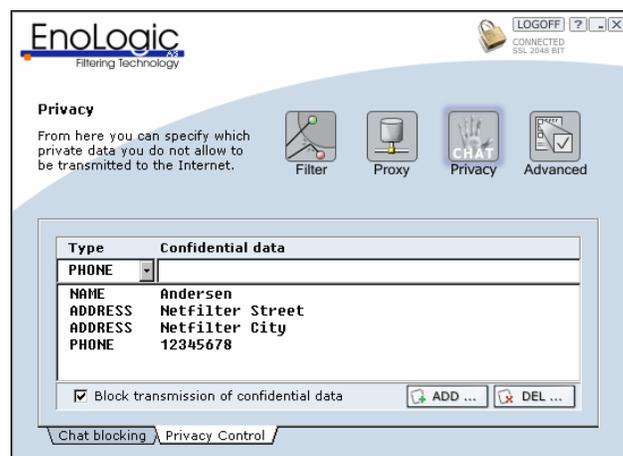


Figure 15: Blocking of transmission of confidential data.

Transmission of confidential data is blocked by, at each keystroke, analysing the text that the user is entering. When the last character of one of the words or numbers in the list is entered, the entered information is deleted and a warning is shown, informing the user that disclosure of personal information is dangerous and therefore not allowed.

The pieces of information that are included in the list should be chosen carefully and should only include information, which is important to protect from disclosure. Consider the following when adding information:

1. Short words and numbers with few digits should be avoided as they can prevent that other, non-personal information can be entered. If, for instance, the name "Theo" is included in the list, it will not be possible to enter the word "theory", as the first part of

this word is identical to the name "Theo".

2. Avoid information that is too specific. For instance, an address could be "17 Netfilter Street", but specifying this address will not prevent the street name "Netfilter Street" from being disclosed. Often, it will be better just to add "Netfilter Street" as address, as this will prevent both the street name "Netfilter Street" and the address "17 Netfilter Street" from being disclosed.
3. Information such as address and telephone number may be abbreviated to the first characters to prevent the first part of the information from being disclosed. For instance, "Netfilter Stree" may be transmitted even though "Netfilter Street" has been added to the list. If "Netfilt" is in the list, however, it is not possible to transmit "Netfilter Stree", but only "Netfil" which may not be enough for the recipient to figure out what the street name is. Note that this use of abbreviations may cause problems if the part of the word that is specified also occurs as a part of other words, as described in item 1.
4. Multiple pieces of information of the same type may be entered. For instance, to pieces of information of the type *Address* may be added, where one contains the street name and the other contains the city name.

Note that it is only possible to add one new piece of information at a time. If, for instance, two telephone numbers are to be added, it is done by first entering one of them, pressing *Add*, and then adding the other.

The filter can only block what is included in the list. It will always be possible to camouflage a piece of information and in that way avoid that the filter blocks the transmission. The filter should mainly be considered a help to remind about the danger of disclosing personal information. Be sure to talk with your children about the dangers of disclosing personal information to strangers on the Internet, where it is easy to pretend to be another person.

3.6. The Advanced Topic

A screenshot from this topic is shown in Figure 16. Here, it is possible to set the more advanced properties, with regard to both EnoLogic NetFilter Admin and EnoLogic NetFilter. The five tabs under the *Advanced* topic make it possible to adjust properties that often can be left unchanged under normal circumstances.

3.6.1 NetFilter Admin Setup

This tab, which is shown in Figure 16, makes it possible to configure properties for EnoLogic NetFilter Admin. It is with the checkbox *Show advanced settings* possible to choose whether the more advanced configuration options are shown. The standard setting is to show the advanced options. If the checkbox is unchecked, the user interface will be simpler but also more limited.

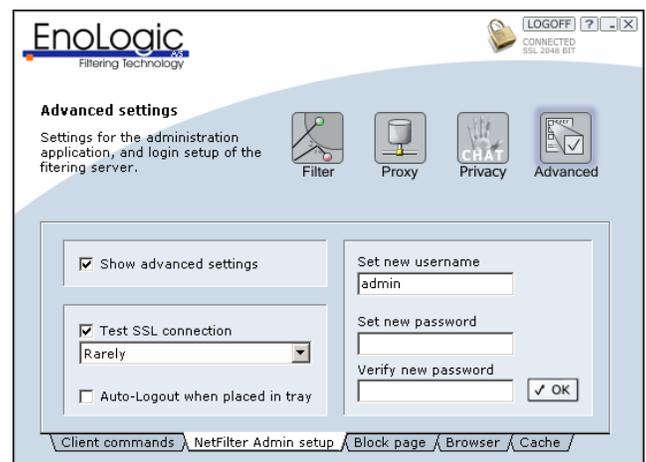


Figure 16: *Advanced settings for EnoLogic NetFilter Admin.*

Using *Test SSL connection* it can be chosen whether EnoLogic NetFilter Admin periodically should check if the encrypted connection between EnoLogic NetFilter Admin and EnoLogic NetFilter is open. Likewise, it is possible to choose how often EnoLogic NetFilter Admin must perform the check. With *Auto-Logout when placed in tray* it is possible to choose whether the program must log of the filtering server when EnoLogic NetFilter Admin is minimized. This is to avoid forgetting to log of when leaving the computer.

If a new username and password is wanted, these can be changed by entering them in the fields to the right in the window. Note that the new password must be entered a second time under *Verify new password* to guard against errors in the entered password. When the *OK* button is pressed, you will be asked to enter your current password. Enter this and press the *OK* button to complete the change of password.

3.6.2 Client Commands

The tab *Client commands*, shown in Figure 17, makes it possible to change the properties of the "blocked page" that appears when it is attempted to access material that the filter classifies as inappropriate. If the field *Enable interactive client commands on the "blocked page"* is checked, any active commands will be included on the blocked page.

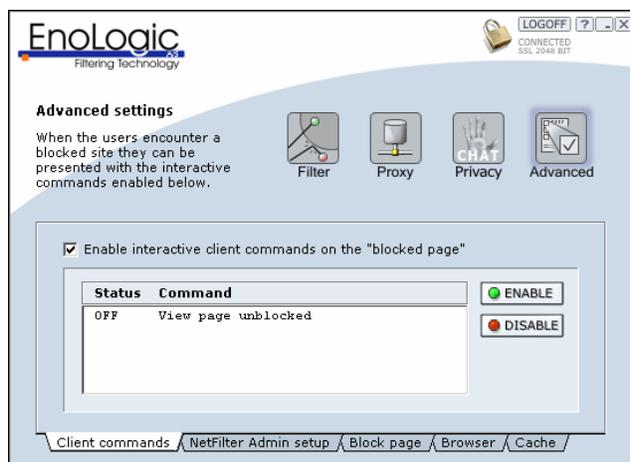


Figure 17: Configuration of Client Commands.

The command *View page unblocked* adds an extra button to the blocked page. This button makes it possible to continue from the blocked page to the material that has been deemed inappropriate. It will be shown on the blocked page that the event is registered in the log file. The command is activated by marking it with the mouse and pressing the *ENABLE* button and deactivated by pressing the *DISABLE* button.

With this command it will be up to the user to decide whether she wants to continue into the page. This may be appropriate if, for instance, a user has a

work-related need to access material that the filter will classify as inappropriate. The user avoids having to contact the system administrator to see the page and can freely continue into the page if she believes it to be relevant for her work.

3.6.3 Block Page

It can, as shown in Figure 18, be changed which language that is used for the block page. It is possible to choose between English and Danish. The block page is the page that is shown instead of the requested page, when EnoLogic NetFilter has found inappropriate material.

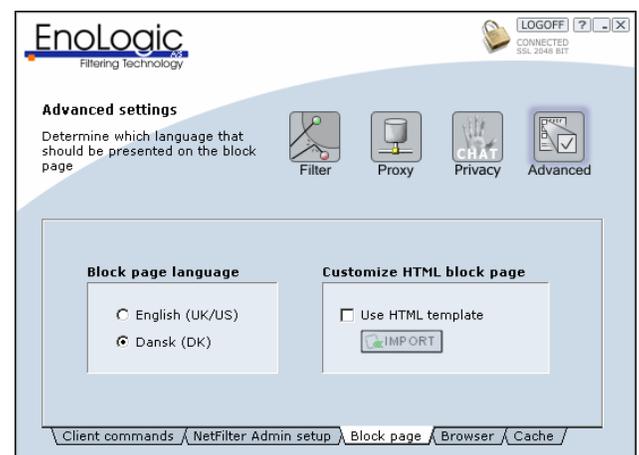


Figure 18: Configuration of block page.

Furthermore, it is possible to replace the standard block page with a page based on a HTML template. This is done by creating a HTML page containing one or more of the following tags:

`[%enologic-netfilter-report%]` – The line with this tag will be replaced with a message stating that the page has been blocked, as well as links for the chosen client commands.

`[%enologic-netfilter-message%]` – The line with this tag will be replaced with a message stating that the page has been blocked.

`[%enologic-imgbtn-view src="IMAGEURL"%]` – The line with this tag will be replaced with a View button. The image at the specified location (IMAGEURL) will be used for the button. The button

will only be shown if the *View page unblocked* client command is active.

`[%enologic-imbbtn-back src="IMAGEURL"%]`
– The line with this tag will be replaced with a Back button. The image at the specified location (IMAGEURL) will be used for the button.

`{%enologic-insert-blocked-url%}` – This tag will be replaced with the URL that was blocked.

`{%enologic-insert-timestamp%}` – This tag will be replaced with the time the page was blocked.

To use the template, it must be imported with the function *Import template* and *Use HTML template* must be checked.

NOTE:

`[%%]` commands replaces the entire line

`{%%}` commands only replaces the tag occurrence

3.6.4 Browser settings

During the installation, the settings in the supported browsers are locked such that the HTTP-traffic is sent through the NetFilter server. If there is a need to modify settings that are not accessible when the browsers are locked, the browsers may be unlocked by removing the checkmark from the field *Lock browser settings*. It is recommended that the browsers are locked again as soon as the settings have been changed. Note that changes in the HTTP proxy settings will be overwritten when the browsers are locked again.

When the field *Optimize IE settings* is checked, Internet Explorer is optimized for use with the NetFilter server. It is recommended that this field is left checked. Change of this setting has effect from the next login or reboot.

3.6.5 Cache

EnoLogic NetFilter stores visited sites in a cache to improve speed when the pages are visited again. You can delete the contents of this cache with the button *Reset*. The numbers above the *Reset* button specifies the memory and disk space used for the cache.

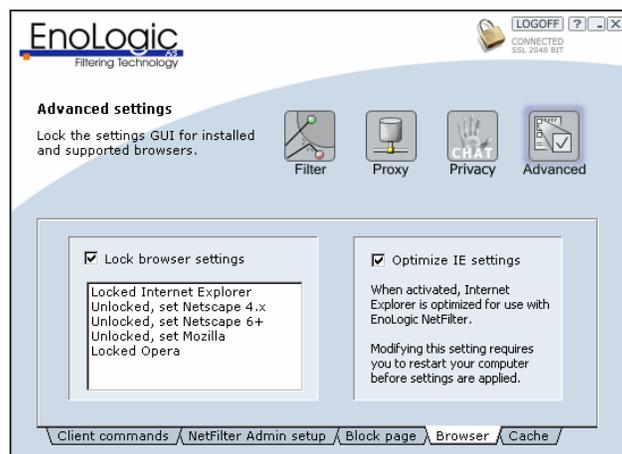


Figure 19: Browser settings.

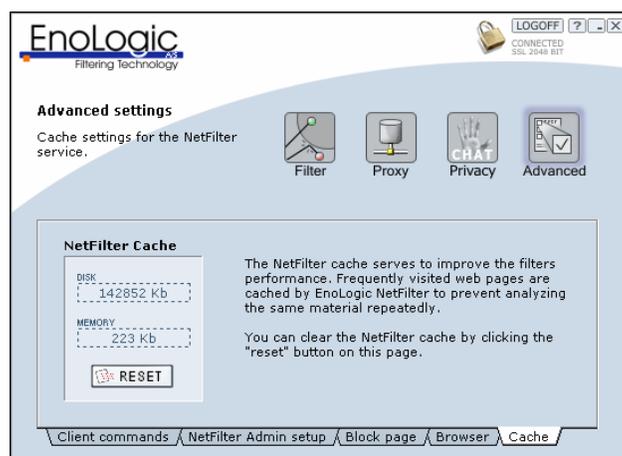


Figure 20: Cache.

4. Automatic updates with EnoLogic NetUpdate

EnoLogic NetUpdate is used for updating the installed EnoLogic product via the Internet. The program is started from the tray icon for EnoLogic NetFilter or from the Start menu. A screenshot from the user interface is shown in Figure 21.

If you are using Windows NT, 2000, or XP, you must be logged in as administrator when you run the program, as it otherwise not always will be possible to perform the updates.

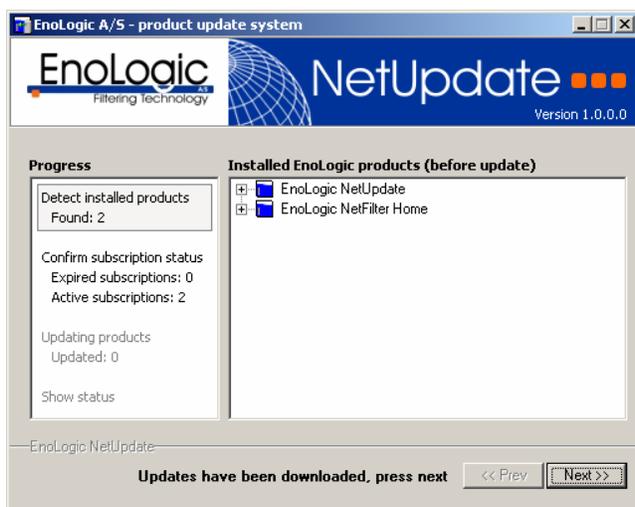


Figure 21: EnoLogic NetUpdate.

5. Uninstallation

EnoLogic NetFilter is uninstalled using the "Add/Remove Programs" function of the Control Panel. Do as follows:

- Open Control Panel.
- Open "Add/Remove Programs"
- Choose "EnoLogic NetFilter Home Trial"
- Press "Remove"

EnoLogic NetFilter will now be uninstalled. If EnoLogic NetUpdate is installed, it may be uninstalled using a similar procedure.

6. Troubleshooting

In this section, some of the problems that may arise when using EnoLogic NetFilter are described.

No Internet connection through EnoLogic NetFilter

If there otherwise is connection to the Internet, the cause of the problem can be that the filter port, which is used for communication between EnoLogic NetFilter and the browsers, is being used by another program on the computer. In this case, EnoLogic NetFilter will inform about the problem when the computer is restarted. The problem can be solved by either

- configuring (or uninstalling) the other program such that it will not use the same port as EnoLogic NetFilter, or
- configuring EnoLogic NetFilter and the browsers to use another filter port, as described in section 3.4.1.

EnoLogic NetFilter Admin cannot establish connection to the EnoLogic NetFilter server

Determine whether another server is using the port, which is used for communication between the EnoLogic NetFilter server and EnoLogic NetFilter Admin. The standard setting is port 9600. If this is the case, the port number for one of the servers must be changed. You can change the port number for EnoLogic NetFilter by creating a text file with the name *ProxyAdminPort.cfg* in the *Data* folder, which is placed in the EnoLogic NetFilter folder, and in this file specify another port number, where after your computer must be restarted. Alternatively, you can stop the other server, log on to the EnoLogic NetFilter server using EnoLogic NetFilter Admin, and set *Admin port* under *Proxy* to another port. (To do this, *Show advanced settings* under *Advanced* must be checked.)

Inappropriate pages are not being blocked

Start EnoLogic NetFilter Admin and check whether filtering is activated (can be seen at the *Status* tab which is shown when the program is started). If not, activate filtering by choosing the tab *Settings* under the topic *Filter* and changing the setting for *Disable filter completely*.

On the tab *Categories* under *Filter*, check whether the category to which the particular pages belong is active. If not, then activate the category.

Check if the particular inappropriate pages are listed in *Granted list*. If necessary, change the settings.

Determine whether the browser is configured to use EnoLogic NetFilter as proxy server. If not, configure the browser with the address and port for the EnoLogic NetFilter server.

If both filter and browser are configured correctly, the cause of this problem may be that the filter misclassifies the particular pages. You can add the

pages to *Always block list* in EnoLogic NetFilter Admin. If the problem is substantial, the sensitivity of the filter may be increased.

Innocent pages are being blocked

Check if the particular pages are listed in *Granted list*. If necessary, change the settings.

In some cases, the content filtering algorithm may fail and classify "innocent" pages as inappropriate. The misclassified pages can be added to the *Always grant list* in EnoLogic NetFilter Admin, causing access to them to be granted always. If the problem is substantial, the sensitivity of the filter may be lowered.

Missing images on the page

This problem may arise for several reasons. If you are using Norton Internet Security and you after the installation of Norton Internet Security have upgraded to Internet Explorer 6, you must install Norton Internet Security again.

If you are using Norton Internet Security, it is important that *EnoLogic NetFilter.exe* have full access to the Internet. This setting may be changed in the administration program for Norton Internet Security, which is shown in Figure 22. The setting for EnoLogic NetFilter should be *Permit All*.

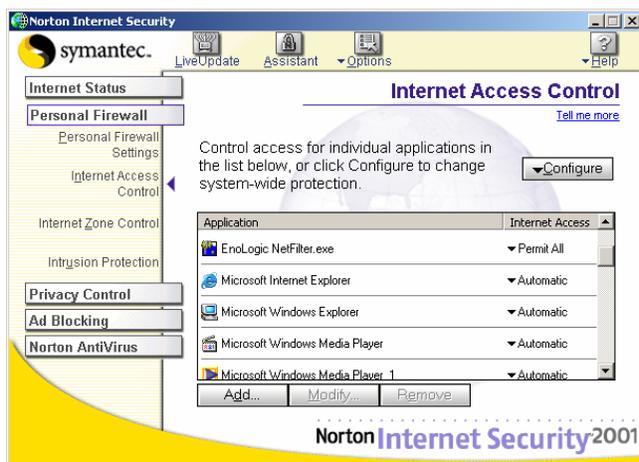


Figure 22: Configuration of Internet access in Norton Internet Security.

Another reason for this problem may be that the browser is not using HTTP 1.1 for communication with NetFilter. For Internet Explorer, this setting may be changed in *Internet Options* under the tab *Advanced*. Use *HTTP 1.1 through proxy connections* must be checked.

The problem may also arise if parts of the configuration for Internet Explorer have been changed such that the communication between the browser and EnoLogic NetFilter does not comply with the standard. These parts of the configuration cannot directly be changed by the user, but may have been changed by another program on the computer. The problem can be fixed by updating the registry with the file *msie_fix.reg*, which is located in Scripts in the installation folder for EnoLogic NetFilter. Right-click on the file and choose *Merge*. This script will also ensure that Internet Explorer uses HTTP 1.1 for communication with NetFilter.

Finally, images may also be missing because they have been blocked by EnoLogic NetFilter, even though the page has not been blocked.

Nothing happens for a long time after requesting a page, then the page is suddenly displayed

When not using EnoLogic NetFilter, web pages are shown progressively as the text and images are downloaded from the Internet. This means you will see part of the page shortly after requesting it (by pressing a link or entering an URL). EnoLogic NetFilter analyses the entire page before passing it on to the browser, as this ensures the highest accuracy possible. Therefore, you will experience a delay. However, the page will then be displayed very quickly as it has been cached by EnoLogic NetFilter. The total amount of time from the page is requested to the entire page has been displayed in the browser will only be slightly higher when EnoLogic NetFilter is used.

The 'Connections'-tab in Internet settings is locked

During the installation, this tab is locked to prevent that the user can deactivate filtering. If you need to change settings available from this tab, it can be unlocked using NetFilter Admin as described in section 3.6.4.

Not possible to modify the proxy settings for the browser

The supported browsers are configured to use EnoLogic NetFilter as HTTP proxy. If you must use a proxy to access the Internet, you may specify the proxy in NetFilter Admin, as described in section 3.4.2. If you in Internet Explorer wish to configure a proxy for another protocol than HTTP, you must first unlock the browser as described in section 3.6.4. Then you will be able to configure Internet Explorer.

7. Customer Service

Updates for the product and answers to frequently asked questions are available from our website:

<http://www.enologic.com>

Technical support is available via e-mail:

E-mail: support@enologic.com

Also see:

<http://www.enologic.com/support/>