

# NetOp<sup>®</sup> Netfilter

*get the full picture*

Version 5.0



## User's Guide



---

Copyright © 1981-2008 Danware Data A/S. All Rights Reserved.  
Portions used under license from third parties.  
Please send any comments to:  
Danware Data A/S  
Bregnerodvej 127  
DK-3460 Birkerød  
Denmark  
Fax: Int +45 45 90 25 26  
E-mail: [info@netop.com](mailto:info@netop.com)  
Internet: [www.netop.com](http://www.netop.com)

---

NetOp® and the red kite are registered trademarks of Danware Data A/S. All other products mentioned in this document are trademarks of their respective manufacturers. Danware Data A/S denies any and all responsibility for damages caused directly or indirectly as a result of using this document. The content of this document is subject to change without notice. Danware Data A/S retains the copyright to this document.

# Contents

<b>1 Introduction .....</b>	<b>6</b>
1.1 Features.....	6
1.2 Contact information.....	7
<b>2 Installing and Uninstalling .....</b>	<b>9</b>
2.1 System Requirements.....	9
2.2 Install on Server.....	10
2.3 Install on Client Computers.....	12
2.3.1 ECLIEN.T.EXE.....	12
2.3.2 Configuration Tool.....	14
2.3.3 Minimal Installation.....	15
2.3.4 Full Installation.....	17
2.3.5 Deploy Clients via A.D.....	20
2.3.5.1 Create Groups.....	20
2.3.5.2 Add Users to Group.....	20
2.3.5.3 Configure 'Netfilter Off' Group Policy.....	22
2.3.5.4 Finish.....	22
2.3.6 Business Desktop Installation.....	22
2.3.7 Hide Tray Icon.....	23
2.4 Uninstall NetOp Netfilter.....	23
2.4.1 Uninstall Client Computers.....	24
2.4.2 Uninstall ECLIEN.T.EXE.....	24
2.4.3 Uninstall Minimal Installation.....	24
2.4.4 Uninstall Full Installation.....	24
2.4.5 Uninstall Server.....	24
2.5 Automatic Updates with NetUpdate.....	24
<b>3 Server Configuration and Supervision .....</b>	<b>26</b>
3.1 Login.....	26
3.2 Navigation in NetOp Netfilter Admin.....	27
3.3 Filter Topic.....	27
3.3.1 Status.....	28
3.3.2 URL Lists.....	30
3.3.2.1 Always Grant List.....	30
3.3.2.2 Always Block List.....	31
3.3.3 Categories.....	32
3.3.4 Peer-2-peer.....	33
3.3.5 Chat Blocking.....	34
3.3.6 Sensitivity.....	35
3.3.7 Setup.....	36
3.3.7.1 General.....	36
3.3.7.2 Network Setup.....	36
3.3.7.3 MP3 Analysis.....	37
3.3.7.4 Large Files.....	38
3.3.7.5 Filename/ext's.....	39
3.3.7.6 Log Setup.....	39
3.3.7.6.1 Segments.....	40
3.3.8 A C L.....	42
3.4 Advanced Topic.....	43
3.4.1 Netfilter Admin Settings.....	43
3.4.2 Client Commands.....	44
3.4.3 Block Page.....	45
3.4.4 Cache.....	46
3.4.5 Time Schedule.....	47
3.4.6 Accounts & Privileges.....	48
3.5 Statistics Topic.....	50
3.5.1 Graphs.....	51
3.6 The Proxy Topic.....	51
3.6.1 Netfilter Proxy.....	52

---

3.6.2 Netfilter Inet-access Proxy .....	52
3.7 Troubleshooting .....	53
3.8 Blacklists.....	54
<b>4 Handling .....</b>	<b>56</b>
4.1 Login page.....	56
4.2 Filters.....	56
4.2.1 Status.....	56
4.2.2 URLs.....	57
4.2.3 Categories.....	57
4.2.4 Peer-2-Peer.....	57
4.2.5 Chat.....	58
4.2.6 Sensitivity.....	59
4.2.7 Setup.....	59
4.2.8 Network Setup.....	61
4.2.9 Segments.....	61
4.2.10 Access Control List.....	62
4.3 Proxy.....	63
4.4 Statistics.....	64
4.5 Advanced Settings.....	64
4.5.1 Interactive client commands.....	64
4.5.2 Netfilter Admin settings.....	65
4.5.3 Block page.....	66
4.5.4 Cache.....	66
4.5.5 Time schedule.....	67
4.5.6 Accounts & Privileges.....	67
<b>Index .....</b>	<b>69</b>

# 1 Introduction

NetOp Netfilter Admin is an administration and maintenance tool for NetOp Netfilter servers. NetOp Netfilter is an advanced Internet filter developed by Danware Data A/S.

If you encounter difficulties using this product, first consult with this user guide. Additional troubleshooting guidance is available at [help.netop.com](http://help.netop.com) in a 'KnowledgeBase' that provide detailed technical information.

The local supplier of your NetOp product is available for advising you on how to obtain maximum benefit from your NetOp product.

As a last resort, you are invited to submit a support request directly to NetOp Support by using the 'Contact Technical Support' form that is available in the 'Support' section of the website [www.netop.com](http://www.netop.com). We will endeavor to get back to you as soon as possible with a solution to your problem.

To read the help pages for Netfilter Admin, see [Handling](#).

For support and contact information, please see the [contact information page](#).

## ***NetOp Support Team***

### **1.1 Features**

Pornography and gambling are thought the fastest growing and most profitable sectors on the Internet.

To companies, the easy access to pornography, gambling and other inappropriate material from the computers of the company can mean decreased productivity, larger load on the company's network, risk of sexual harassment and damage to the corporate image.

Schools and libraries, which are offering pupils and users access to the Internet, have a moral obligation to protect minors against inappropriate material, and at the same time they have an obligation to ensure that the access to the Internet is not used for violations of the copyright of, among other things, music, movies and software. By filtering the Internet access with NetOp Netfilter, irrelevant and illegal use of the Internet can be reduced significantly.

NetOp Netfilter can block inappropriate content on the Internet within the following categories:

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

The core of NetOp 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. The administrator can specify whether the users can continue to such pages, or if they only are permitted to return to the previous

page. If a user chooses to continue to the page in spite of the warning, it is registered in a log file.

NetOp Netfilter can also block chat and peer-2-peer file sharing programs, 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.

NetOp Netfilter works as a proxy server for HTTP traffic. This ensures compatibility with almost all web browsers on all operating systems.

NetOp Netfilter can be used by itself, as illustrated in Figure 1, or together with an external proxy server, as illustrated in Figure 2. The possibility to couple NetOp Netfilter with a third-party proxy server ensures smooth integration of NetOp Netfilter in an existing network.

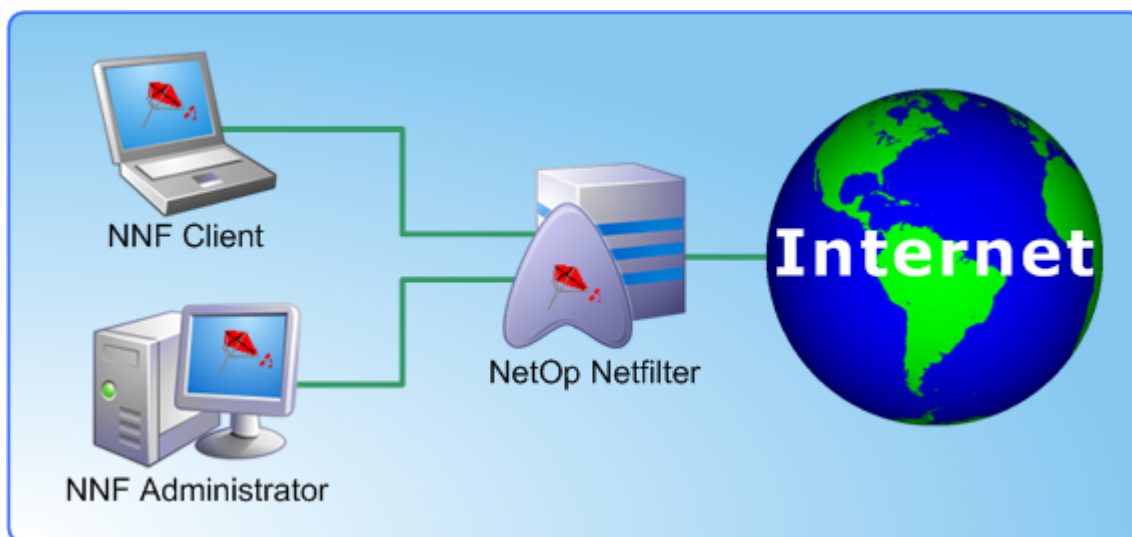


Figure 1: Use of NetOp Netfilter without a third-party proxy server.

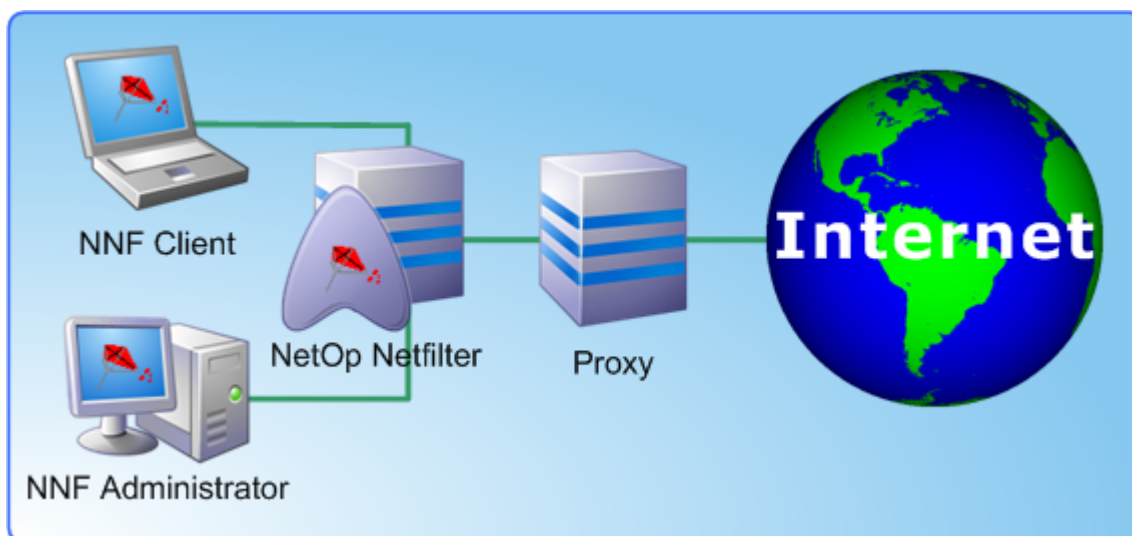


Figure 2: Use of NetOp Netfilter together with an external proxy server.

## 1.2 Contact information

### Customer service

Technical support, including answers to frequently asked questions, is available from our website:

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

### Contact information

Mailing address:

Danware Data A/S

Bregnerodvej 127

3460 Birkerød

Denmark

Email: [info@netop.com](mailto:info@netop.com)

Web: <http://www.netop.com>

## 2 Installing and Uninstalling

The installation of NetOp Netfilter consists of two steps. First, NetOp Netfilter must be installed on a server with Internet access. Then, the client computers for which the Internet traffic must be filtered must be configured to use NetOp Netfilter as proxy server.

[System Requirements](#)

[Install on Server](#)

[Install on Client Computers](#)

[Uninstall NetOp Netfilter](#)

[Automatic Updates](#)

[Hide Tray Icon](#)

### 2.1 System Requirements

#### Server

Minimum requirements:

- 700 MHz Pentium-compatible CPU
- 128 MB RAM
- 50 MB of free space on the hard disk
- Microsoft Windows NT 4, Windows Server 2000/2003 all server editions

The behaviour of the users is significant for the requirements for the server. If the users are "average users", who mainly visit non-pornographic sites and rarely download large files, the number of hits pr. second that they produce in peak load periods may be used for estimating the requirements for the server hardware, using Figure 3.

If the number of hits pr. second is known, for instance if a proxy is already being used, this number may be used to determine the requirements for the Netfilter server.

If the numbers are not known, it may be assumed that an average user produce 1 hit/sec. when browsing on the Internet. For instance, if the peak load is when 100 computers are being used for surfing at the same time, 100 hits/sec. will be produced.

1 hit/sec. is an average number for an entire session. The hits will appear in burst that may include more than 50 hits over a period of 1-2 seconds from a single user. The server must be able to handle this load to ensure an acceptable delay for each user.

CPU (MHz)	Hits/sec	Throughput (Mbps)
700	80	4
1333	120	6
2200	160	8

**Figure 3: Performance at different CPU speeds. As the hardware requirements depend on the behaviour of the users, these number should only used as a guide.**

**Note:** Figure 3 is based on an assumption of 0% cache hits. In reality, the number of cache hits will typically be in the range 10-50%. Thus, a server with a given processor will be able to handle a larger load than specified in the table.

If the load from the network is larger than what a single server can handle, it is necessary to employ several servers. The clients on the network must in this case be configured to use different proxy server, such that the traffic is distributed between the servers.

As the Internet connection limits the bandwidth available to the users, the requirements for the server may also be determined using the speed of the Internet connection by comparison with the throughput column in Figure 3.

It is important to note that the filter introduces a delay. To ensure an acceptable delay for each user, it is recommended that at least a 700 MHz server is used.

### Clients

All browsers that can use a HTTP proxy are, in principle, supported. The included client configuration software can automatically configure the following browsers:

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

The client configuration software supports:

Microsoft Windows 98, ME, NT 4, 2000, XP and Vista

Linux

Mac OS

## 2.2 Install on Server

### Installation

To install the program, click the link provided by Danware.

You can either select *Run* or *save*.

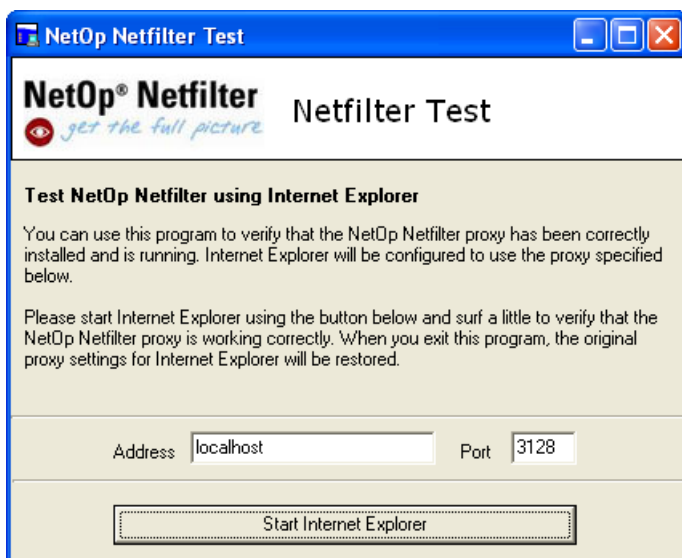
If you select *Run*, the installation will commence at once. If you select *Save* the installation file has to be activated to begin installation.

The installation program will lead you through the steps necessary for the installation of NetOp Netfilter. After the installation has been completed, NetOp Netfilter is installed as a service and will be started automatically.

The default TCP-port which NetOp Netfilter utilizes for browser communication is 3128. If another port is needed, e.g. if port 3128 is already in use by another application on the machine, this can be changed easily with the NetOp Netfilter Admin program which is described in [Netfilter Proxy](#).

### First execution

Before the clients in the network are configured to utilize NetOp Netfilter, it should be examined if NetOp Netfilter is configured correctly and has access to the Internet. If the port for browser communication has not been changed and Internet Explorer is installed on the machine, it can easily be verified with the NetOp Netfilter Test application, shown in Figure 4. Start the application and start Internet Explorer afterwards by clicking the *Start Internet Explorer* button. If NetOp Netfilter is configured correctly, the browser will show a page with a message stating that NetOp Netfilter is installed correctly. Try visiting a page on the Internet to verify you can connect to the Internet.



**Figure 4: NetOp Netfilter Test.**

Alternatively, you can open a browser and set the proxy server to the IP-address/machine name of the machine where NetOp Netfilter is installed and the port number to 3128 (unless another port has been chosen in NetOp Netfilter Admin). If the browser is running on the same machine as NetOp Netfilter, it is sufficient to enter *localhost* as machine name. In English/US versions of Internet Explorer 5 and higher, choose the menu:

Tools > Internet Options > Connections > LAN settings

Mark the checkbox Use a proxy server. Enter IP-address/machine name of NetOp Netfilter in the Address field and 3128 in the Port field, as shown in Figure 5. If the browser is opened on the same machine as NetOp Netfilter, enter *localhost* as address. The checkbox *Bypass proxy server* for local addresses must be unchecked.

To verify that NetOp Netfilter is installed and configured correctly, enter

`http://are-you-alive`

in the Address field in the browser. A correctly configured NetOp Netfilter will show a message, stating that NetOp Netfilter is correctly installed. You can also visit a page on the Internet, to make sure the server is correctly connected to the Internet.

If a page is not shown correctly, it is important to examine if the page is working without NetOp Netfilter in a browser which is not configured to use NetOp Netfilter. This should be done to make sure that the Internet page is not temporarily offline.

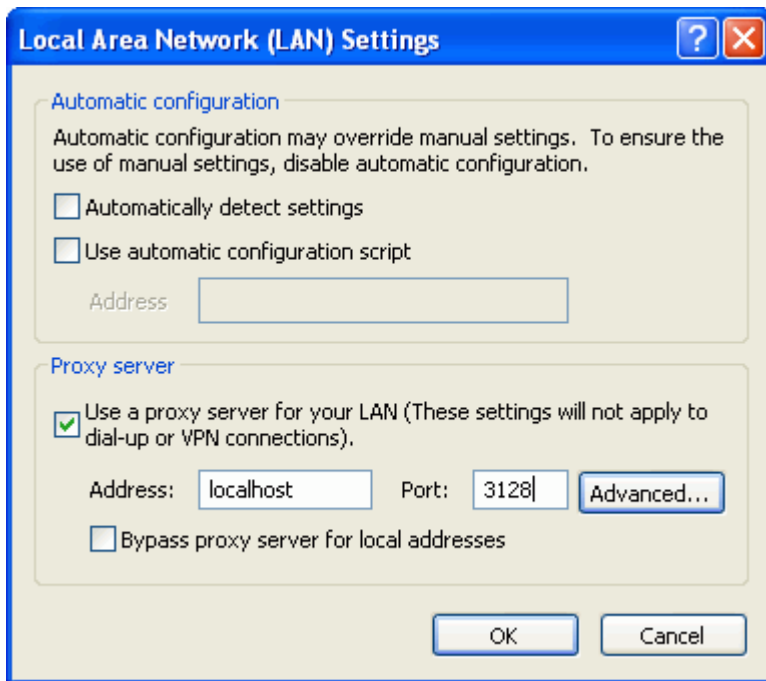


Figure 5: Configuration of proxy.

See: [Server requirements](#).

## 2.3 Install on Client Computers

Filtering is enabled by configuring the web browsers to use the NetOp Netfilter server as a proxy server for HTTP traffic. If the client computers are running Microsoft Windows 98, ME, NT 4, 2000, XP or Vista, this can be done using ECLIENT or Configuration Tool, which also lets you configure user interface restrictions that prevent users from modifying the settings.

If you are using automatic proxy configuration on your network, the most convenient way to enable filtering will be to change the proxy address and port in the configuration script. If you have access to tools for remote administration of browser settings, such as policies or Netscape Mission Control Desktop, you may also use these.

If you already use a proxy on you network, but is not using automatic proxy configuration (and do not wish to begin doing it), you can also enable filtering by configuring NetOp Netfilter to run on the same address and port as the proxy you currently use, and move your proxy to another port and/or address (if you still wish to use it). In that way, you do not have to change the settings on the client computers.

See: [Client requirements](#), [ECLIENT.EXE](#), [Configuration Tool](#), [Minimal Installation](#), [Full Installation](#), [Deploy Clients via Active Directory](#) and [Hide Tray Icon](#)

### 2.3.1 ECLIENT.EXE

ECLIENT.EXE can be used to modify the proxy settings for Internet Explorer. It may be used in a logon script as an alternative to a .reg-file from *Configuration Tool*. ECLIENT.EXE support Windows 98, ME, NT, 2000, XP and Vista.

Furthermore, ECLIENT.EXE must be running on the clients to make it possible to use user name logging, peer-2-peer blocking, and chat blocking. If these features are not needed, there is no need to have ECLIENT.EXE running on the clients.

**Note:** If user name logging is activated, ECLIENT.EXE must be running on all clients or ECLIENT.EXE must be running with the parameter [/sharedip](#) and support for shared IP must be activated in Netfilter Admin, as the Internet access otherwise will become very slow for the

clients not running ECLIEN.T.EXE. Do not activate user name logging before ECLIEN.T.EXE is running on all clients.

If you have a mixed network with, for instance, Windows 95, 98, XP, and Macintosh computers, you may still use user name logging for the supported machines. However, it is important that you use /sharedip. That way, the Internet access will not be slow for clients that do not run ECLIEN.T.EXE.

The following parameters can be used with ECLIEN.T.EXE:

- /usernamehost=addr Name or IP address of the server to be used for user name logging. If Netfilter is installed only on one server, it is the address of this that must be specified here. If user name logging is not used, this parameter may be omitted.
- /blockhost=addr Name or IP address of the server that settings for chat and peer-2-peer blocking must be retrieved from. If Netfilter is installed only on one server, it is the address of this that must be specified here. This parameter may be omitted if chat and peer-2-peer blocking is not used.
- /proxyhost=addr Name or IP address of the server to be used for filtering. If Netfilter is installed only on one server, it is the address of this that must be specified here. If this parameter is not specified, ECLIEN.T.EXE will not modify the proxy settings.
- /proxyport=nnnn Port number for Netfilter's [Filter Port](#). If this parameter is not specified, the port is assumed to be 3128, which is the default setting for Netfilter.
- /script=url Address of proxy script. Use this parameter if the proxy settings are controlled by a script.
- /autodetect Use automatic proxy detection.
- /bypass=list List of addresses that Netfilter should not be used for. Traffic to these addresses are not directed through Netfilter, i.e. it must be possible for the clients to access the specified addresses directly. The addresses in the list are separated with semicolon (;).
- /local Specify this parameter if Netfilter also must be used as proxy for traffic to addresses on the local network.
- /disableproxy Specify this parameter to disable use of proxy, e.g. when uninstalling.
- /nolock If this parameter is specified, the user interface for modifying the proxy settings will not be locked, i.e. the user will still be able to modify the proxy settings (unless the user interface is locked in another way).
- /unlock Specify this parameter to unlock the user interface. Used when uninstalling.  
Must be specified if several users share the same IP address. This is the case if Citrix or Terminal Services is used or if there is another proxy server between the users and NetOp Netfilter. If /sharedip is not specified in these cases, the traffic will not be logged correct. User name logging and support for shared IP address must be activated as described in [Log Setup](#).
- /sharedip

**Note:** When /sharedip is used, correct logging of the traffic requires that all users use Internet Explorer as browser.

ECLIEN.T.EXE may be run from the logon script of the users. To do this, the program must first be copied to a location on the network that is accessible to all clients. ECLIEN.T.EXE is found under Client in the folder where NetOp Netfilter has been installed, typically:

```
\\Program Files\Danware Data\NetOp Netfilter\ Business\Client
```

When ECLIENT.EXE has been copied to an appropriate location, a line must be added to the logon-script which runs ECLIENT.EXE with the desired parameters, for instance:

```
\\myserver\files\eclient.exe /unamehost=10.10.10.10 /  
proxyhost=10.10.10.10
```

**Note:** The text above must be placed on a single line.

The program will now be started each time a user logs on and set the proxy settings such that the specified server is used as proxy.

If local firewalls are installed on the clients, it is important that these are configured to permit ECLIENT.EXE to function as a server and to access the Internet.

**Note:** The lists with peer-2-peer and chat programs that must be blocked are updated once every half hour, that is, up to 30 minutes may pass before changes made with the administration program become active on all clients.

### 2.3.2 Configuration Tool

If you wish to use Configuration Tool for configuration of the client computers, the program can be started from the Start menu:

```
Start > Programs > NetOp NetFilter > Business > Configuration Tool
```

The program will lead you through the steps that are necessary to configure the proxy settings and user interface restrictions. As shown in Figure 6, you will be offered the choice between Minimal installation using registry script and Full installation using setup program.



**Figure 6: Choice of Configuration Mode.**

Choose [Minimal installation](#) if you wish to configure the clients using a .reg file with the settings for Microsoft Internet Explorer. If the users share a logon script, minimal installation is the most convenient, but minimal installation only supports Internet Explorer. No software is installed on the client computers by minimal installation.

Choose [Full installation](#) if you wish to configure the clients using a setup program, which must be executed on each computer that is to use filtering. Software will be installed on the client computer that corrects the settings for the users when they log on, if they deviate from the settings chosen in Configuration Tool. This software also configures browsers that are installed after the installation of the filter has been completed.

If you wish to use user name logging, peer-2-peer blocking and chat blocking, the program [ECLIENT.EXE](#) must be running on the client computers. ECLIENT.EXE may be run from the logon-script of the users.

Press *Next* when the desired configuration mode has been chosen. The two configuration modes are described in detail in the following sections.

### 2.3.3 Minimal Installation

You will first be asked to enter the address of the machine which NetOp Netfilter is installed on and the port number that is used by NetOp Netfilter. Unless you have chosen another in NetOp Netfilter Admin, the port number is 3128. Enter this information on the page shown in Figure 7. It is also possible to specify whether communication with local addresses (that is, other machines on the intranet) is to be filtered by NetOp Netfilter, and it is possible to specify a list of servers for which the traffic should not be filtered (for instance, your own web server).

“Bypass Netfilter for Hotmail addresses” must be checked to make access to Hotmail from Outlook possible. If it is checked, traffic to addresses containing “hotmail” and “services.msn” will not be sent through Netfilter. This makes it possible to access Hotmail from Outlook, but at the same time it means that pages with these addresses will never be analyzed/blocked by the filter. It is not necessary to bypass Netfilter for these addresses to make Hotmail access from browsers possible.

Configuration tool

**NetOp® Netfilter** *get the full picture* Netfilter Configuration Tool

**Specify the address and port of the NetOp Netfilter server**

The address can be specified as a name or an IP address. The default port number used by the NetOp Netfilter server is 3128.

Server

Address:  Port:

Bypass Netfilter for local addresses

Bypass Netfilter for Hotmail addresses (required for Hotmail access from Outlook)

Do not use Netfilter for addresses beginning with:

Use semicolons [ ; ] to separate entries.

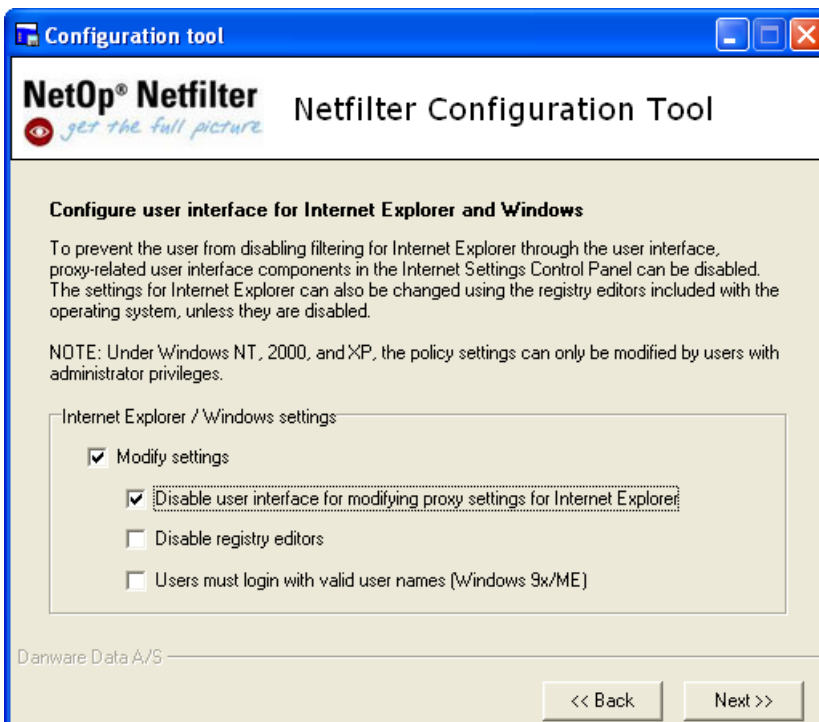
Danware Data A/S

<< Back      Next >>

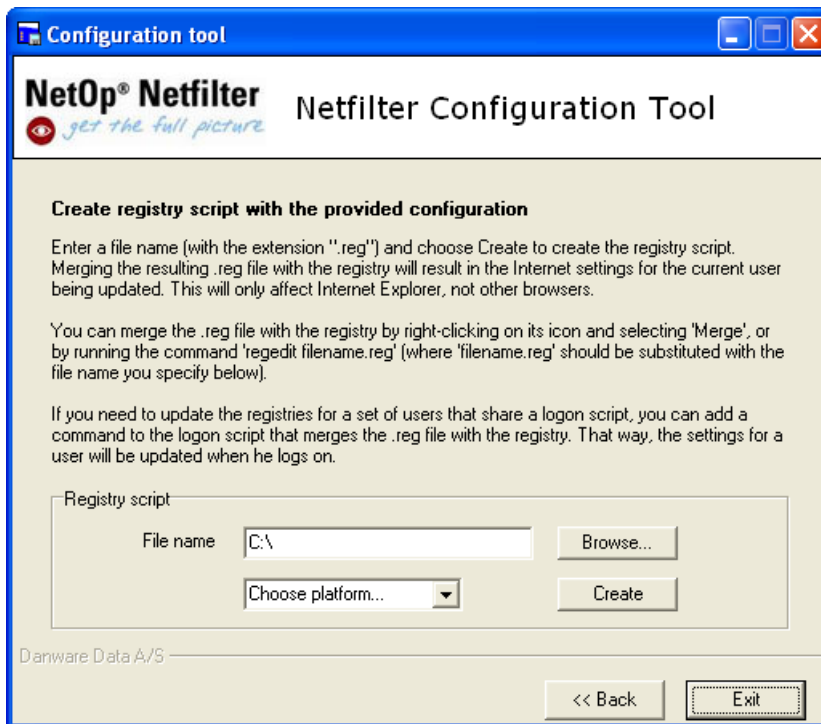
**Figure 7: Entry of Proxy Settings.**

With minimal installation, it is in general only possible to configure user interface restrictions for client computers that are running Windows 98 or ME. On computers that are running Windows NT, 2000, XP or Vista, only the proxy settings can be configured in this way. Therefore, the page for configuration of user interface restrictions, shown in Figure 8, should only be used for configuring clients running Windows 98 and ME. In this case, you can specify on this page that the user should not be able to change the proxy settings in Internet Explorer. Furthermore, it is possible to disable tools for modification of the registry (regedit and regedt32) which also can be used for modifying the proxy settings for Internet Explorer. Under Windows 98 and ME, it is usually possible for the user to log in without specifying a user name by pressing ESC when the login prompt is displayed. This is not desirable when user names are logged. To ensure that the user logs in with a valid user name, the option Users must login with valid user names can be checked.

The last step in Configuration Tool for minimal installation is generation of a .reg file with the chosen configuration. The page for this step is shown in Figure 9. Here, a name for the .reg file must be entered. Then, Create is pressed to generate the file. Configuration tool can now be closed with the button Exit.



**Figure 8: Configuration of User Interface Restrictions.**



**Figure 9: Creation of .reg File.**

The .reg file that Configuration Tool has produced must now be used to update the settings on the client computers.

If the users share a logon scripts, you can update the settings from the script. This can be done by inserting the command

```
regedit /s reg_file
```

in the logon script, where reg\_file is the path to and name of the .reg file.

You can also update the registry manually for a user by right-clicking on the icon of the .reg file and choosing Merge.

### 2.3.4 Full Installation

You will first be asked to enter the address of the machine which NetOp Netfilter is installed on and the port number that is used by NetOp Netfilter. Unless you have chosen another in NetOp Netfilter Admin, the port number is 3128. Enter this information on the page shown in Figure 10. It is also possible to specify whether communication with local addresses (that is, other machines on the intranet) is to be filtered by NetOp Netfilter, and it is possible to specify a list of servers for which the traffic should not be filtered (for instance, your own web server).

“Bypass Netfilter for Hotmail addresses” must be checked to make access to Hotmail from Outlook possible. If it is checked, traffic to addresses containing “hotmail” and “services.msn” will not be sent through Netfilter. This makes it possible to access Hotmail from Outlook, but at the same time it means that pages with these addresses will never be analyzed/blocked by the filter. It is not necessary to bypass Netfilter for these addresses to make Hotmail access from browsers possible.

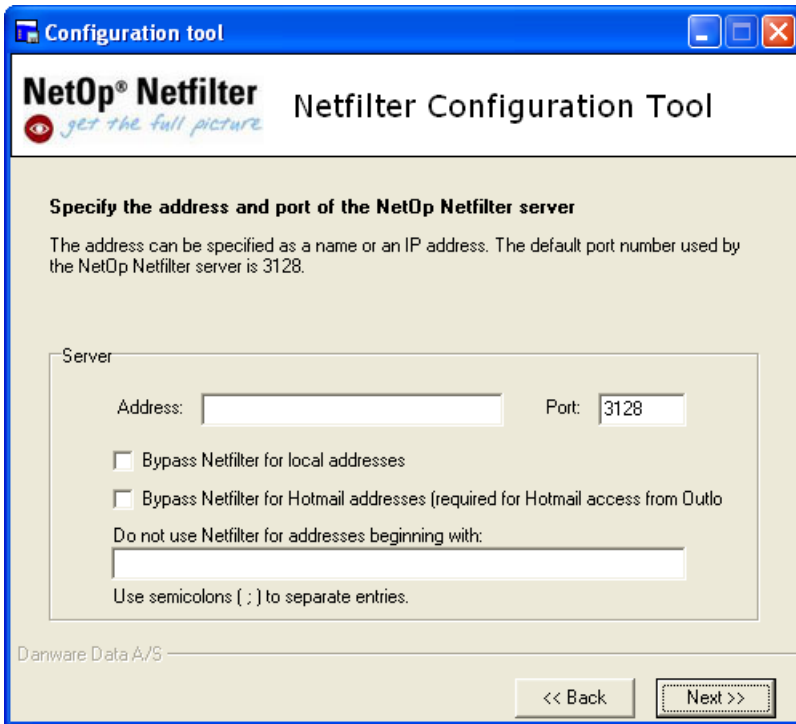


Figure 10: Entry of Proxy Settings.

After entering the proxy settings, it is possible to configure user interface restrictions, see Figure 11. These restrictions make it more difficult for the user to modify the proxy settings and thereby avoid filtering.

Under Windows 98 and ME, it is usually possible for the user to log in without specifying a user name by pressing ESC when the login prompt is displayed. This is not desirable when user names are logged. To ensure that the user logs in with a valid user name, the option Users must login with valid user names can be checked.

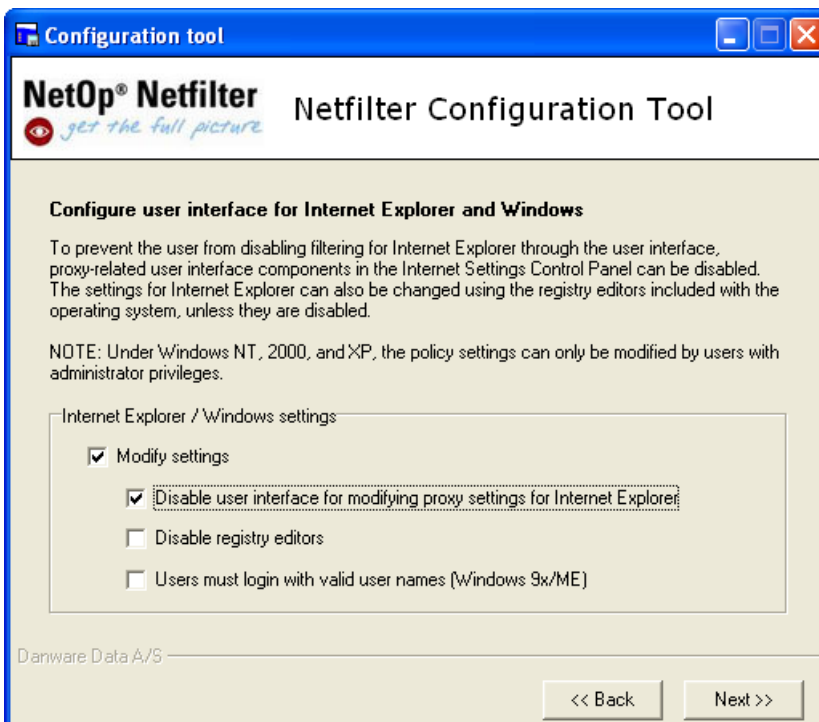
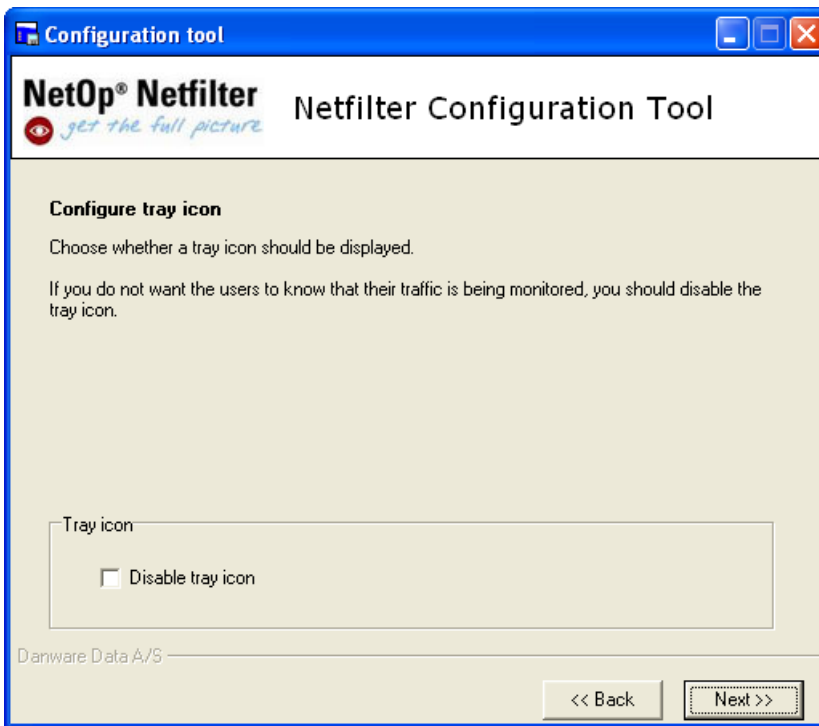


Figure 11: Configuration of User Interface Restrictions for Internet Explorer and Windows.



**Figure 12: Deactivation of tray icon.**

On the next page, shown in Figure 12, the tray icon for Netfilter can be deactivated, for instance to avoid that the users can see that their Internet traffic is being analyzed.

When the user interface restrictions have been configured, the program is ready to produce a setup disk. This is done on the page shown in Figure 13, where a location must be chosen and it must be specified which version of Windows that the client machines are using.

The location for the setup disk does not necessarily have to be a floppy disk. You can also choose another location for the setup files, for instance a network drive that is accessible from the client computers that must be configured. When a location for the files has been chosen, Create is pressed to produce the setup disk. Configuration Tool will now create the necessary setup files on the chosen location. To configure a client computer, the file CLISETUP.EXE on the setup disk must be run on the computer.

**Note:** Under Windows NT, 2000, XP and Vista, CLISETUP.EXE must be run with Administrator privileges.

If CLISETUP.EXE is run with the parameter `"/verysilent"`, no user interface is shown. This can be utilized when performing an automatic installation, e.g. from a logon-script, but be aware that the program must be run with Administrator privileges if the operating system is Windows NT, 2000, XP or Vista. To ensure that CLISETUP.EXE is only run once, it may be checked whether one of the files that are installed already exists on the computer, for instance

```
%ProgramFiles%\NetOp\Configuration Manager\ Configuration Manager.exe
```

To uninstall, CLISETUP.EXE must be run with the parameter `"/uninstall"`. This may be combined with `"/verysilent"` to hide the user interface.

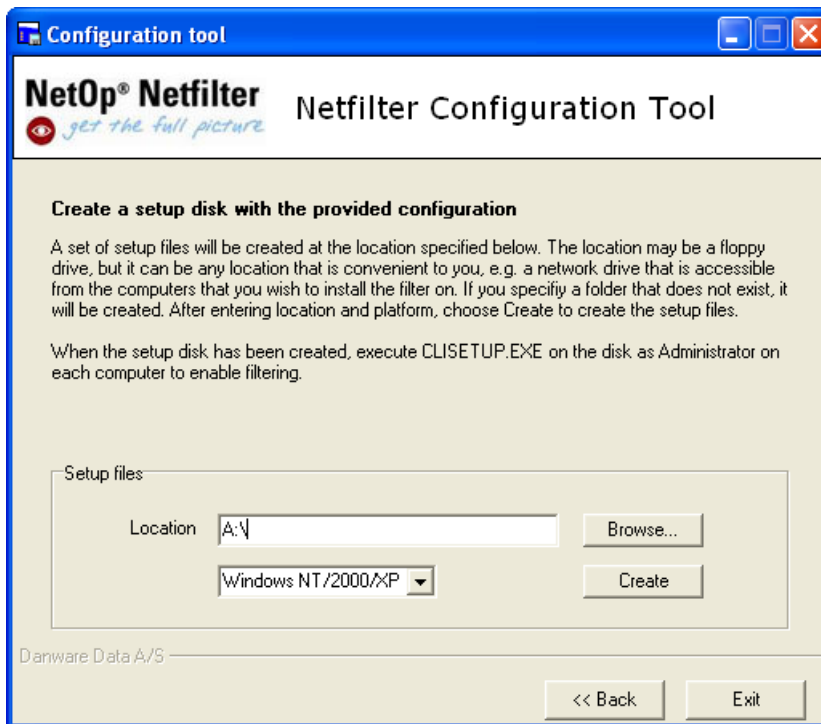


Figure 13: Creation of Setup Disk.

## 2.3.5 Deploy Clients via A.D.

This section describes how to use group policies to activate NetOp Netfilter for selected users while, optionally, leaving other users unfiltered in a Windows environment using Active Directory for user management.

NetOp Netfilter operates as a proxy server. To activate Netfilter for a user, this user's browsers must be configured to use Netfilter as proxy when accessing the web. The steps outlined below will do this for Microsoft Internet Explorer.

See: [Install on Client Computers](#), [Create Groups](#), [Add Users to Group](#), [Configure 'Netfilter Off' Group Policy](#) and [Finish](#)

### 2.3.5.1 Create Groups

1. Open Active Directory Users and Computers, which is available from the Start menu.
2. Locate the domain containing the users that must have their Internet traffic filtered. If users from several domains must be filtered, you may repeat the steps below for each domain.
3. Create, in this domain, two groups of users: **FilteredUsers** and **UnfilteredUsers**.
4. A group is created by right-clicking on the container and choosing *New > Group* in the pop-up menu. The group type should be Security and the scope Domain local.

### 2.3.5.2 Add Users to Group

1. Add all users that are to use the Netfilter proxy to FilteredUsers and all other users to UnfilteredUsers. You can add users to a group by
  - double-clicking on the group and choosing the members on the Members tab in the group properties window,
  - double-clicking on the person to add a choosing the group on the Member of tab in the user properties window, or

- choosing the users, right-clicking on one of them and choosing Add members to a group.

### Create "Netfilter On" Group Policy

2. Open the properties window for the domain by right-clicking on the domain and choosing Properties. Go to the Group Policy tab.

3. Add and name Group Policy:

- Click *New* to add a new group policy and name it **Netfilter On**.
- Open the properties window for this policy by clicking on the Properties button. In the properties window, go to the Security tab. Choose the group *Authenticated Users* and remove the checkmark in the Allow column for *Apply Group Policy*.
- Click *Add* to add a new group. A new window opens. Choose the group *FilteredUsers* and press *Add*, then *OK*.
- Back on the Security page, check the *Allow* checkbox for *Apply Group Policy*. Click *OK*.

4. Create "Netfilter Off" Group Policy

- Click *New* to add a new group policy and name it **Netfilter Off**.
- Open the properties window for this policy by clicking on the *Properties* button. In the properties window, go to the *Security* tab. Select the group *Authenticated Users* and remove the checkmark in the *Allow* column for *Apply Group Policy*.
- Click *Add* to add a new group. Choose the group *UnfilteredUsers* and press *Add*, then *OK*.
- Back on the *Security* page, check the *Allow* checkbox for *Apply Group Policy*. Click *OK*.

5. Configure "Netfilter On" Group Policy

- Double-click on the *Netfilter On* policy. This will open the *Group Policy* snap-in.
- Go to *User Configuration > Windows Settings > Internet Explorer Maintenance > Connection* and double-click on *Proxy Settings*.
- Check *Enable proxy settings* and enter the address and port of the Netfilter proxy in the HTTP fields. Uncheck *Use the same proxy server for all addresses*. If you use one or more proxies for the other types of traffic, the addresses and ports of these should be entered in the other fields. Configure *Exceptions* as desired. Note that if *Do not use proxy server for local (intranet) addresses* is checked, web pages on your intranet will not be filtered. Click *OK* to return to the *Group Policy* window.
- If you use automatic browser configuration on your network, you should disable this for the users in the *FilteredUsers* group. Do this by double-clicking on *Automatic Browser Configuration* and unchecking *Automatically detect configuration settings* and *Enable Automatic Configuration*.
- To prevent users from modifying proxy settings (and thereby avoiding filtering), go to *User Configuration > Administrative Templates > Windows Components > Internet Explorer*.
- Double-click on *Disable changing proxy settings* and set the value to *Enabled*. You may want to do the same for *Disable changing Automatic Configuration settings*, *Disable changing connection settings*, and/or *Disable Internet Connection wizard*.
- Go to *User Configuration > Administrative Templates*. Right-click on *Administrative Templates* and choose *Add/Remove Templates*. This will result in a new window being opened. Choose *Add* and open the file **netfilter.adm**, which is located in the *Scripts* subdirectory in the directory that NetOp Netfilter was installed to. Then click *Close* to return to the group policy window.
- In the group policy window, the entry *User Configuration > Administrative Templates > NetOp Netfilter* has now appeared. Left-click, then right-click on NetOp Netfilter and make sure that the option *View > View Policies Only (\*)* is not checked. Then double-click

on Internet Explorer settings and enable the policy. Click *OK* to accept the default settings. (Use HTTP 1.1 through proxy connections should be checked for the best performance. It is recommended to use the default values for the Max. connections... entries, but increasing the values may decrease the delays experienced when surfing through the proxy. However, if the values are too high, requests from the browser will be lost and the users will experience missing images on the web pages.)

\*) In Windows Server 2003, the View Policies Only option has been moved to a dialog, which you open by choosing View > Filtering... in the menu. The name of the option has changed to Only show policy settings that can be fully managed.

- Close the *Group Policy* snap-in.

### 2.3.5.3 Configure 'Netfilter Off' Group Policy

1. Double-click on the *Netfilter Off* policy. This will open the *Group Policy* snap-in.
2. Go to *User Configuration > Windows Settings > Internet Explorer Maintenance > Connection* and double-click on *Proxy Settings*.
3. Configure the proxy settings as desired, giving either direct access to the Internet (when Enable proxy settings is not checked), or access through a proxy server.
4. If you use automatic browser configuration on your network, you may need to enable this for the users in the UnfilteredUsers group. Do this by double-clicking on *Automatic Browser Configuration* and checking *Automatically detect configuration settings* and/or *Enable Automatic Configuration* and fill out the other information as desired.
5. To undo the changes done [here](#) preventing users from modifying proxy settings (if a user is moved from the FilteredUsers group to the UnfilteredUsers group), go to *User Configuration > Administrative Templates > Windows Components > Internet Explorer*.

Double-click on *Disable changing proxy settings* and set the value to *Disabled*. You may want to do the same for *Disable changing Automatic Configuration settings*, *Disable changing connection settings*, and/or *Disable Internet Connection wizard*. Close the *Group Policy* window.

### 2.3.5.4 Finish

Close the domain properties window and the *Active Directory Users and Computers* window. The users you added to the FilteredUsers group will now use the Netfilter proxy when accessing the web (they may have to login again before the new policy is applied).

If a user in the FilteredUsers group must have unfiltered access to the Internet, simply remove him from the FilteredUsers group and add him to the UnfilteredUsers group, instead. Please note that just removing him from the FilteredUsers group may not be sufficient to change whether he uses the Netfilter proxy – he must be added to the UnfilteredUsers group for the proxy settings to be changed. Similarly, you can remove a user from the UnfilteredUsers group and add him to the FilteredUsers group to activate filtering for this user.

### 2.3.6 Business Desktop Installation

Install *NetOp Netfilter Business Desktop* on mobile personal computers on which you want *NetOp Netfilter* protection while not connected to the *NetOp Netfilter* protected network.

#### Automatic Installation

1. Create a group named *Business Desktop* as explained in [Create Groups](#).
2. Apply the *Netfilter On* group policy to *Business Desktop* as explained in [Add Users to Group](#).
3. In the *Netfilter On* group policy under *Computer Configuration > Administrative Templates >*

*NetOp Netfilter*, enable *Business Desktop settings*. Specify the *NetOp Netfilter* server address as the *Address of Netfilter server*. *Business Desktop* will contact the server to exchange settings and log files.

4. Copy the installation package *NetOp Netfilter Business Desktop.msi* from the *Program Files > Danware Data > NetOp Netfilter > Business > Client* folder to a shared folder that is accessible from the mobile personal computers on which it shall be installed.

5. In the *Netfilter On* group policy, right-click *Computer Configuration > Software Settings > Software Installation* and select *New > Package*. Select the shared folder installation package and click *Open*. Select *Advanced* and click *OK*.

6. On the *Deployment* tab, select *Assigned* and *Install this application at logon*. This will install the *Business Desktop* package on network computers when their user logs on.

7. To update installations from an updated installation package, overwrite the shared folder installation package. In the *Netfilter On* group policy under *Computer Configuration > Software Settings > Software Installation*, right-click *NetOp Netfilter Business Desktop* and select *All tasks > Redeploy application*.

### Manual Installation

1. In the computer registry under the key *HKEY\_LOCAL\_MACHINE\SOFTWARE\EnoLogic\NetFilter\Business*, write the *NetOp Netfilter* server address to a *REG\_SZ* value named *ServerName*.

2. Run the installation package *NetOp Netfilter Business Desktop.msi* on the computer.

### Hide Tray Icon

By default, the *NetOp Netfilter* icon will be shown in the system tray in the lower right corner of the screen.

To hide it by a group policy, in the *Netfilter On* group policy under *Computer Configuration > Administrative Templates > NetOp Netfilter* double-click the *Hide tray icon* policy and select *Enable*. This will have effect from the next user login.

## 2.3.7 Hide Tray Icon

When the Client has been installed a Netfilter icon is shown in the System Tray.

This icon can for various reasons be disabled, meaning that the Client runs in stealth mode (invisible to the user).

**Warning:** In some countries the user has to be able to see whether he or she is being monitored. Please, check with local laws and labor law.

To activate the tray icon in Business Desktop via Active Directory, follow these steps:

1. Go to *Computer Configuration > Administrative Templates > NetOp Netfilter*
2. Double-click the *Hide tray icon* and
3. Set it to *Enabled*.

The changes will be effective from the next time the user logs on.

See: [Add Users to Group](#)

## 2.4 Uninstall NetOp Netfilter

If you wish to uninstall NetOp Netfilter, but still wish to use a proxy server, you may skip the uninstall of the clients, and let the proxy server run on the address and port, which was used for NetOp Netfilter. Otherwise, it is recommended that the uninstall first is done on the clients, as there otherwise will not be HTTP access to the Internet from these until the uninstall has been completed.

**Note:** From the *Add or Remove Programs* section in Windows it is also possible to *Repair NNF*

Business Administration. The most important feature here is the possibility to reset Username and Password.

### 2.4.1 Uninstall Client Computers

How the uninstall of NetOp Netfilter is done depends on whether you have done a minimal or full installation. The information, which is presented here, is only relevant if you have used Configuration Tool for the installation.

### 2.4.2 Uninstall ECLIENT.EXE

If ECLIENT.EXE is used to set the proxy settings, the logon-script is modified such that it reads:

```
\\myserver\files\eclient.exe /disableproxy /unlock
```

This will deactivate use of proxy and unlock the user interface. When all users have logged in, the line may be removed from the logon script. If you have been using the /nolock parameter, you may omit /unlock from the line above.

### 2.4.3 Uninstall Minimal Installation

If you have done a [Minimal Installation](#), filtering on the client computers can be disabled using a .reg file, which restores the original settings. If the original settings are the standard settings for Windows / Internet Explorer, one of the files NETFILTER\_9X\_OFF.REG or NETFILTER\_NT\_OFF.REG can be used. They are placed in the Scripts folder in the installation folder for NetOp Netfilter, which is typically *\Program Files\Danware Data\NetOp Netfilter\Business*. For client computers which use Windows 98 or ME, the file NETFILTER\_9X\_OFF.REG must be used, while NETFILTER\_NT\_OFF.REG must be used for client computers running Windows NT, 2000, XP or Vista.

### 2.4.4 Uninstall Full Installation

The client software is uninstalled by running CLISETUP.EXE on the setup disk with the parameter "/uninstall", see [Full Installation](#). It may be necessary to reboot the computer to complete the uninstall, but no message will be shown indicating this and it will not happen automatically.

After uninstalling, the traffic from this client will no longer be filtered.

### 2.4.5 Uninstall Server

The server software is uninstalled using the "Add/Remove Programs" function of the Control Panel. Do as follows:

- Open Control Panel.
- Open "Add/Remove Programs" Choose "NetOp Netfilter"
- Press "Remove"

NetOp Netfilter will now be uninstalled.

## 2.5 Automatic Updates with NetUpdate

NetUpdate is used for updating the installed NetOp product via the Internet. The program is started from the tray icon for NetOp Netfilter or from the Start menu.

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

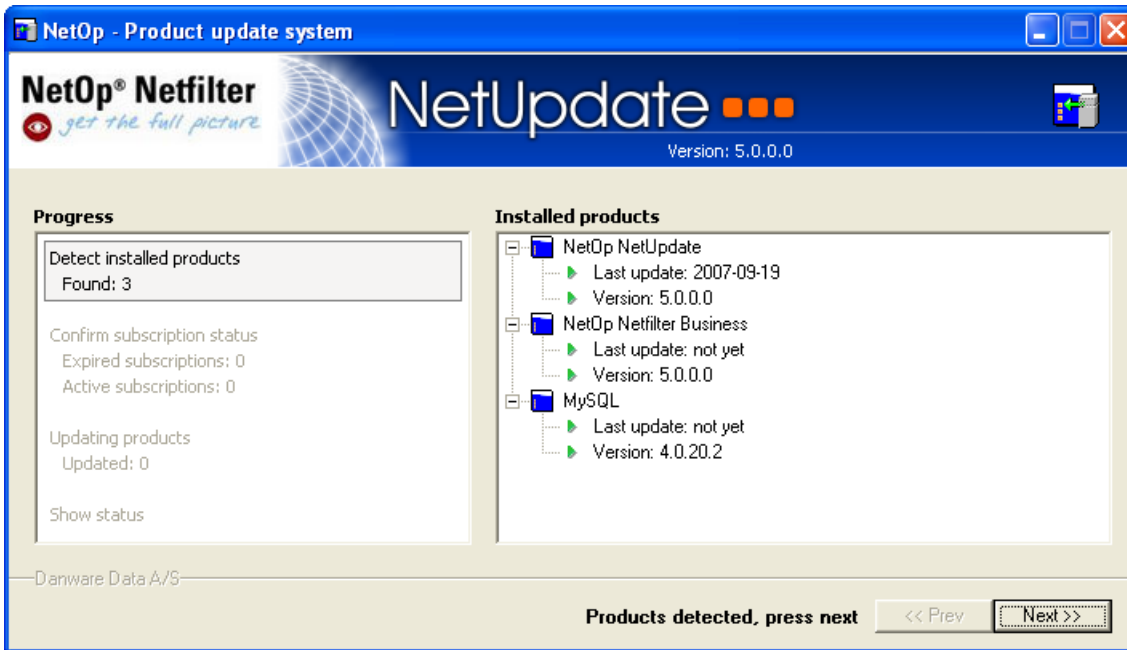


Figure 44: NetUpdate.

## 3 Server Configuration and Supervision

The settings for NetOp Netfilter can be changed with the program NetOp Netfilter Admin, which also shows statistics for the traffic through the filter. NetOp Netfilter Admin can be started from the Start menu:

```
Start > Programs > NetOp Netfilter > Business > Netfilter Admin
```

NetOp Netfilter Admin can be run locally on a filtering server, that is, a server that NetOp Netfilter is running on. It is also possible to perform remote administration from another computer on the network by starting NetOp Netfilter Admin on this machine. In the case of remote administration, the IP address of the filtering server to administrate must be known.

[Login](#)

[Navigation in NNF Admin](#)

[Troubleshooting](#)

[Filter Topic](#)



[Advanced Topic](#)



[Statistics Topic](#)



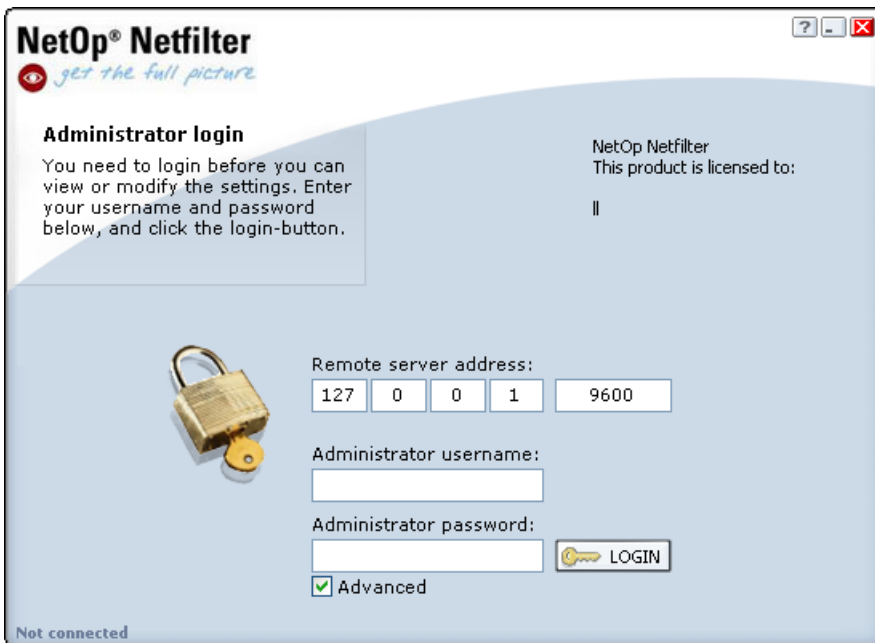
[Proxy Topic](#)



### 3.1 Login

When NetOp Netfilter Admin is started, a login window as shown in Figure 14 will appear. In this window, the IP address of the filtering server must be specified together with the number of the administration port for NetOp Netfilter.

If NetOp 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 NetOp 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 NetOp 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 [Netfilter Proxy](#).



**Figure 14: Filtering Server Login.**

To strengthen security 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 NetOp Netfilter Admin is started, both the username and the password are "admin".

When the username and password have been entered, the Login button is pressed. If the login at the filtering server is successful, a screen as shown in Figure 15. will appear. If the login is not successful, an error message is shown instead.

See: [Troubleshooting](#)

## 3.2 Navigation in NetOp Netfilter Admin

After a successful login, a start page as shown in [Figure 15](#) 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 NetOp Netfilter Admin. The [Filter topic](#) is activated after login. 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](#).

See: [Troubleshooting](#)

## 3.3 Filter Topic

The Filter topic contains information and standard configuration options for NetOp Netfilter. The different tabs for Filter are described in the following sections.

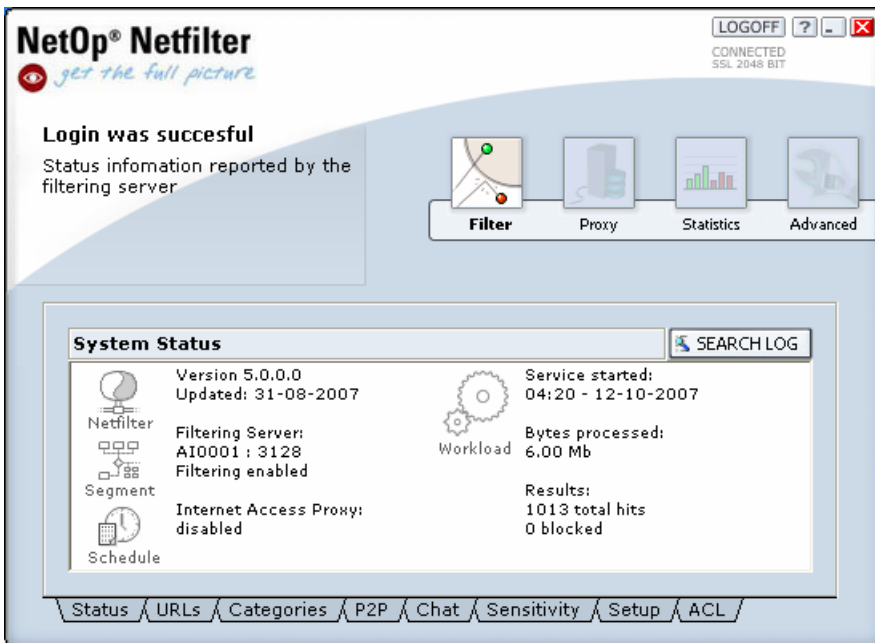


Figure 15: Status-page which is shown after login.

See: [Troubleshooting](#)

### 3.3.1 Status

The tab [Status](#) makes it possible to see information regarding NetOp Netfilter. As it can be seen in [Figure 15](#), it is possible to read:

- The version number for NetOp 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 possible to be presented to at detailed statistics by pressing the button SEARCH LOG. This will open a browser with a statistics page showing granted and blocked traffic through the filter.

The statistics include:

- Distribution of blocked traffic on categories.
- Distribution of granted/blocked traffic over time.
- Distribution of MP3 and large file transfers over time.
- Distribution of bandwidth consumption over time.
- Activity analysis that for each machine shows amount of traffic and estimated time spent for both granted and blocked traffic.
- List of blocked pages that the user has chosen to view in spite of the warning.

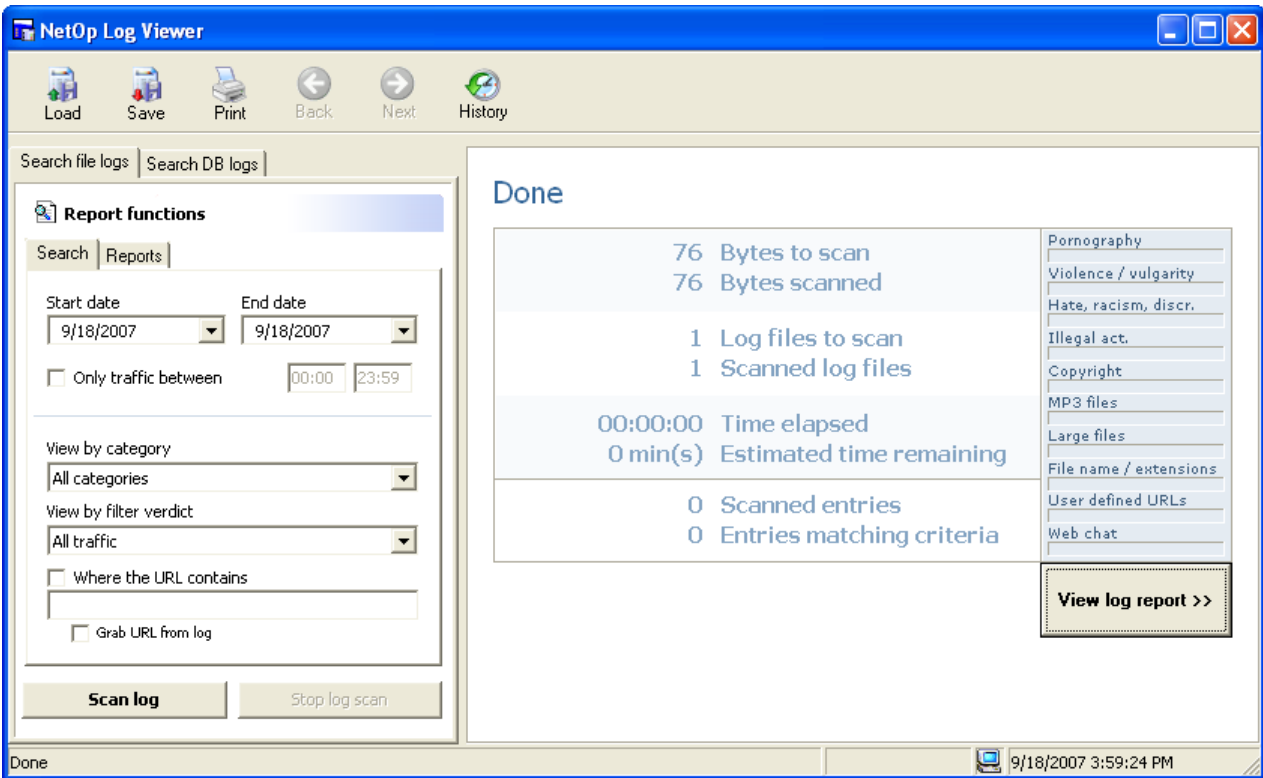


Figure 16: Searching in log files.

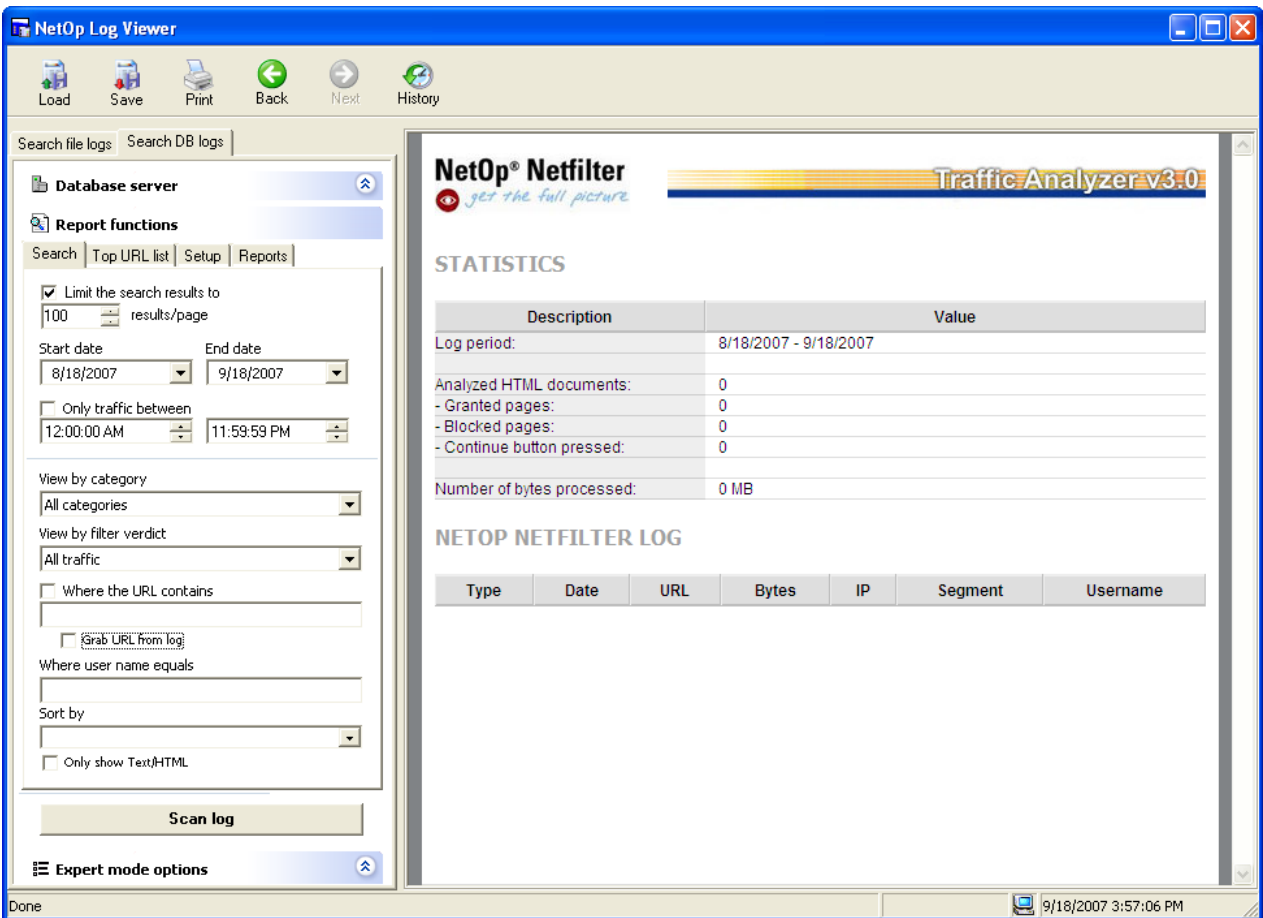



Figure 17: Searching in database.

The SEARCH LOG button will open a window that lets you search for entries in the log that match certain criteria, such as date, time, category, and URL. NetOp Netfilter can log traffic to either local log files on the server or to a database. As shown in [Figure 16](#) and [Figure 17](#), it is possible to choose between searching the local log files or the database.

When searching in log files, the search criteria shown in [Figure 16](#) can be used. Note that the panel with search criteria is “unfolded” using the icon  in the upper right corner. The search is started with the button Scan log. Searching in log files may be slow and should be limited to the necessary entries using the search criteria. During the search, information showing the progress is displayed. When the search is done, the report may be shown using the View log report button.

When searching in a database, similar search criteria are available and it is possible to have the results displayed on pages with e.g. 100 entries at each, making it possible to see results before all entries have been searched.

Advanced users can under Export mode options choose to have a SQL editor shown which makes it possible to customize the search. The SQL code is updated automatically, when the search criteria are changed. Start the search with the Scan log button.

IP addresses are stored in a special format in the database. To translate an address from the usual notation for IP addresses to this format, the SQL editor’s IP Calculator may be used. It is started with the IPCALC icon. The two small disk-icons make it possible to save and load SQL code.

It is possible to change address, name, etc. for the database using the Database server panel.

Using the buttons at the top of the window, it is possible to print or save the current report or load a previously saved report. To switch between different pages, the buttons Back and Next may be used. It is also possible to switch between pages by clicking in the history that is shown at the bottom of the window when the History button has been pressed.

See: [Troubleshooting](#)

### 3.3.2 URL Lists

URLs are the addresses of web-pages. Some of these pages' content is inappropriate - others not. The URLs can be organized in lists:

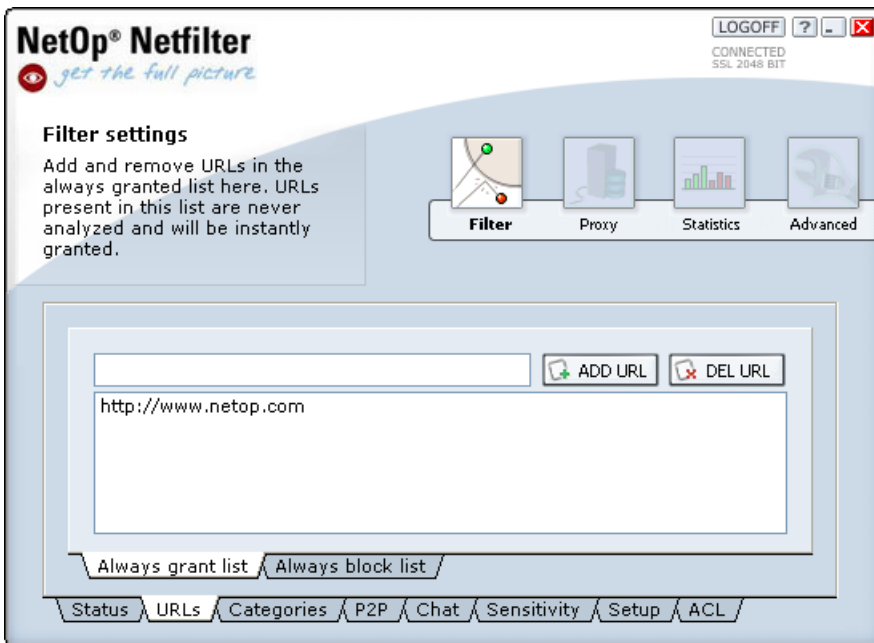
See: [Troubleshooting](#), [Always Grant List](#) and [Always Block List](#)

#### 3.3.2.1 Always Grant List

The tab Always grant list, which can be seen in [Figure 18](#), makes it possible to add URLs that should never be blocked by NetOp Netfilter, no matter their content. This makes it possible to add, for instance, the company’s internal web server, such that it will not be analysed.

To add an URL, enter it in the URL field and click ADD URL.

To remove an URL, select an URL and click DEL URL.



**Figure 18: Always grant list. The addresses in this list will never be blocked.**

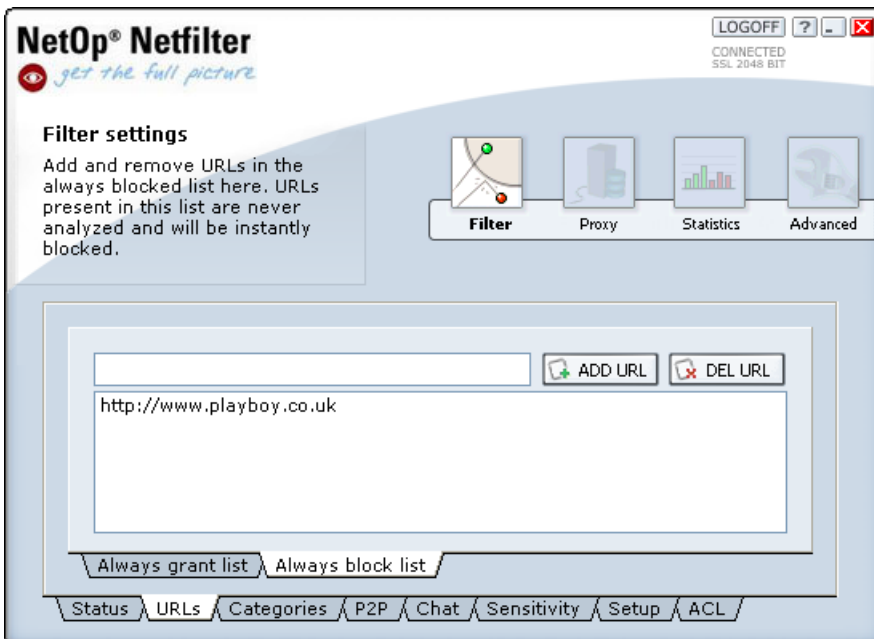
An URL in the grant list covers all sub-URLs. For instance, access to `http://www.netop.com/test/` will always be granted with the settings shown in Figure 18. Inversely, `http://www.test.com` could be blocked even though `http://www.test.com/dirty/` has been added to the list.

### 3.3.2.2 Always Block List

The tab Always block list, shown in Figure 19, makes it possible to add URLs that no matter their content must be blocked. This makes it possible to add pages that are not covered by the categories, for instance, gambling or other unwanted material.

To add an URL, enter it in the URL field and click ADD URL.

To remove an URL, select an URL and click DEL URL.



**Figure 19: Always block list. The addresses in this list will always be blocked.**

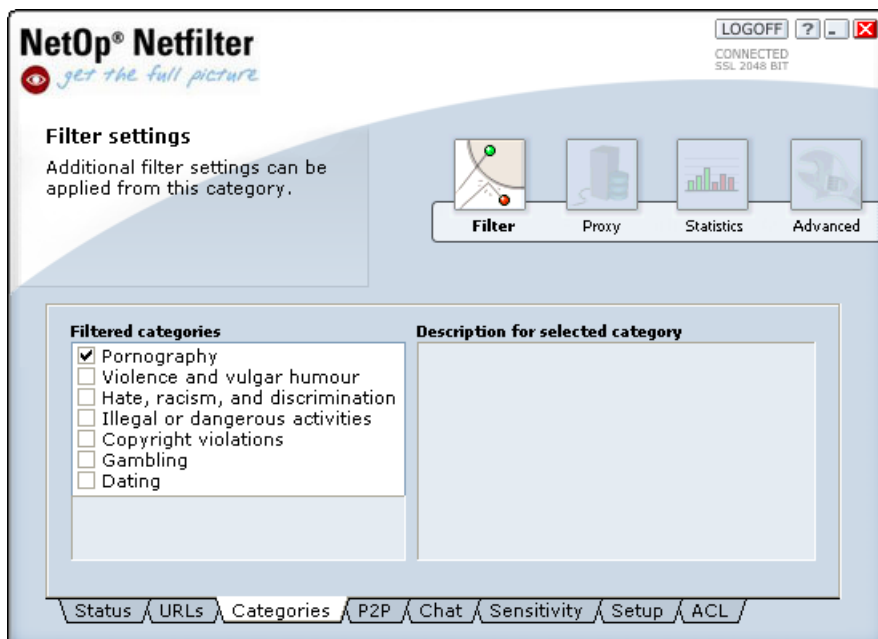
An URL which is specified in the block list covers all sub-URLs. For instance, <http://www.gambling.com/test/> will always be blocked with the settings shown in Figure 19. Inversely, <http://www.test.com> may be granted even though <http://www.test.com/dirty/> has been added to the list.

### 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 20. 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.
- Dating. Pages offering dating services, such as personal ads and speed dating, as well as marriage agencies.
- Gambling. Pages related to gambling. Sites that let users gamble for money, such as online casinos and bookmakers, are the primary target, but this category also includes sites offering related information, such as gambling instructions, gambling-related software, sports statistics, and the web sites of casino resorts.
- 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 humor. 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 20: Categories.** The filter blocks the categories chosen in the list.

See: [Setup Categories](#) and [Troubleshooting](#)

### 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.

**Note:** Peer-2-peer blocking can only be used if [ECLIEN.T.EXE](#) is running on the clients.

In the [list](#) to the left in Figure 21, 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.

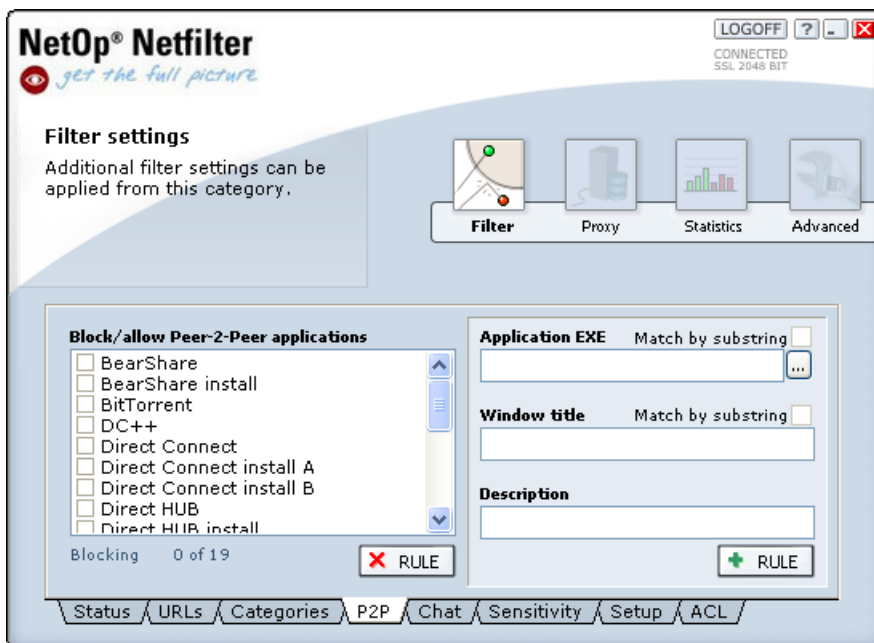
If you right-click on the list, a menu with the following functions is displayed:

- 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.



**Figure 21: Blocking of peer-2-peer programs.**

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 [deleted](#) from the list by selecting it and pressing XRULE. The programs in the built-in list cannot be removed.

See: [Troubleshooting](#)

### 3.3.5 Chat Blocking

The page for chat blocking is shown in Figure 22. 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.

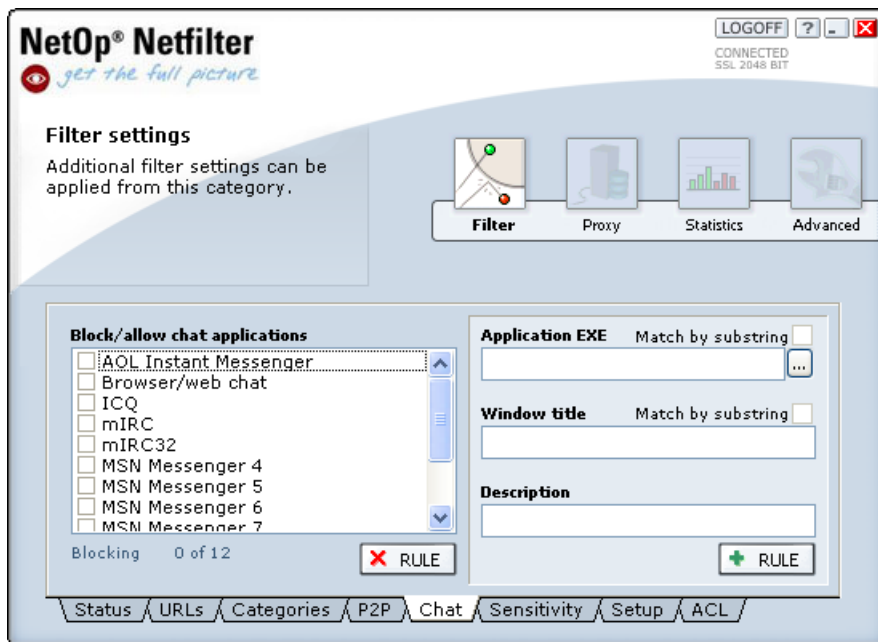


Figure 22: Chat blocking.

**Note:** Blocking of chat programs can only be used if [ECLIENT.EXE](#) is running on the clients. Browser/web chat blocking can always be used, though.

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.

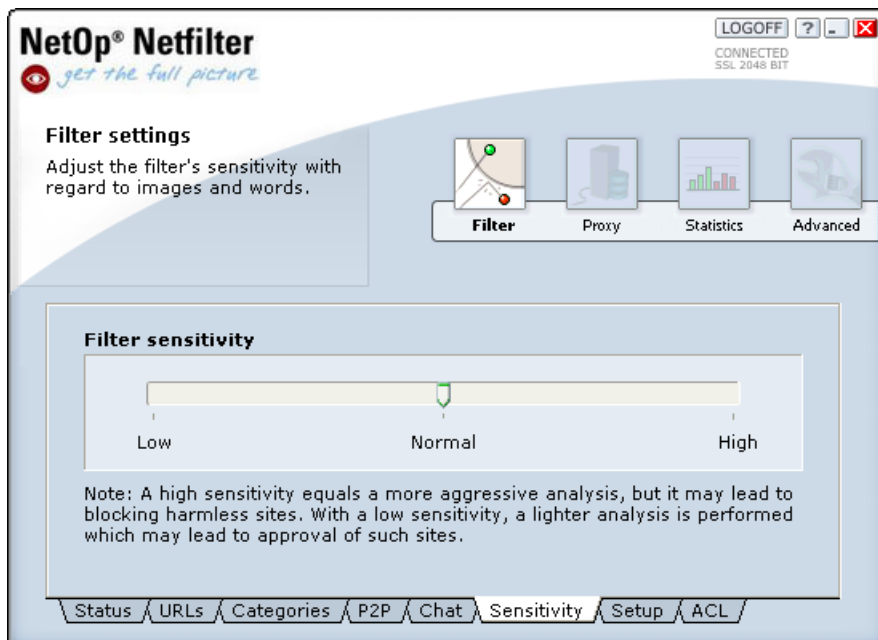
The blocking works by closing the programs. Some seconds may pass before this happens. If the window title is used for matching, the program is only closed if the window is active.

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.

See: [Troubleshooting](#)

### 3.3.6 Sensitivity

As shown in Figure 23, the tab Sensitivity makes it possible to [adjust the sensitivity](#) of NetOp Netfilter with regard to inappropriate material. It is possible to choose between three settings for sensitivity, [Low](#), [Normal](#), and [High](#).



**Figure 23: Adjustment of the sensitivity of the filter.**

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.

See: [Troubleshooting](#)

### 3.3.7 Setup

The tab Setup 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.

See: [Filter Setup](#), [General](#), [Network Setup](#), [MP3 Analysis](#), [Large Files](#), [Filename/ext's](#) and [Log Setup](#)

#### 3.3.7.1 General

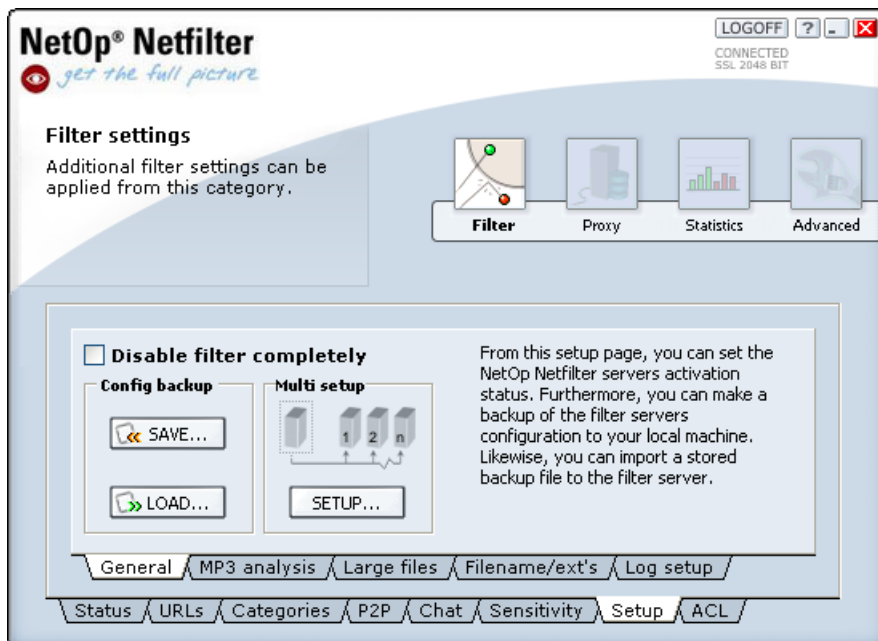


Figure 24: General settings for the filter.

- [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.
- Config backup. This makes it possible to save a copy of the configuration in a local file and later load it to restore the configuration.
- [Network setup](#). Makes it possible to send the current setup to a number of other servers over the network.

See: [Setup General](#).

#### 3.3.7.2 Network Setup

With [Network Setup](#) it is possible to manage a number of Netfilter servers at the same time. It is done by customizing the settings on one server and then transferring the settings of this server to the rest. The servers that the settings must be sent to are added to the list in [Figure 25](#). Then Apply is pressed to send the settings to the specified servers.

[Proxy settings](#) are only sent to the other server if *Also copy proxy settings* is checked.

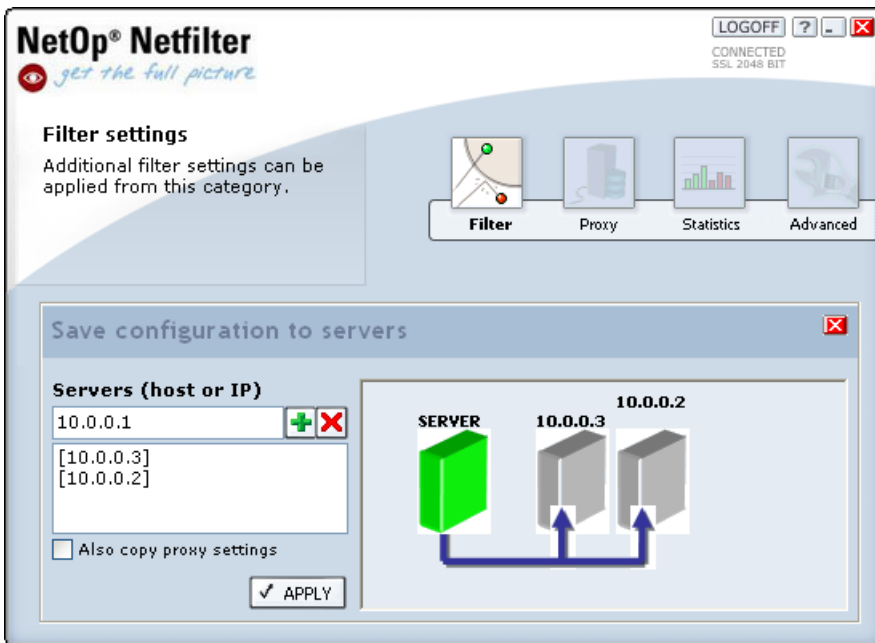


Figure 25: Network Setup.

See: [Network Setup](#).

### 3.3.7.3 MP3 Analysis

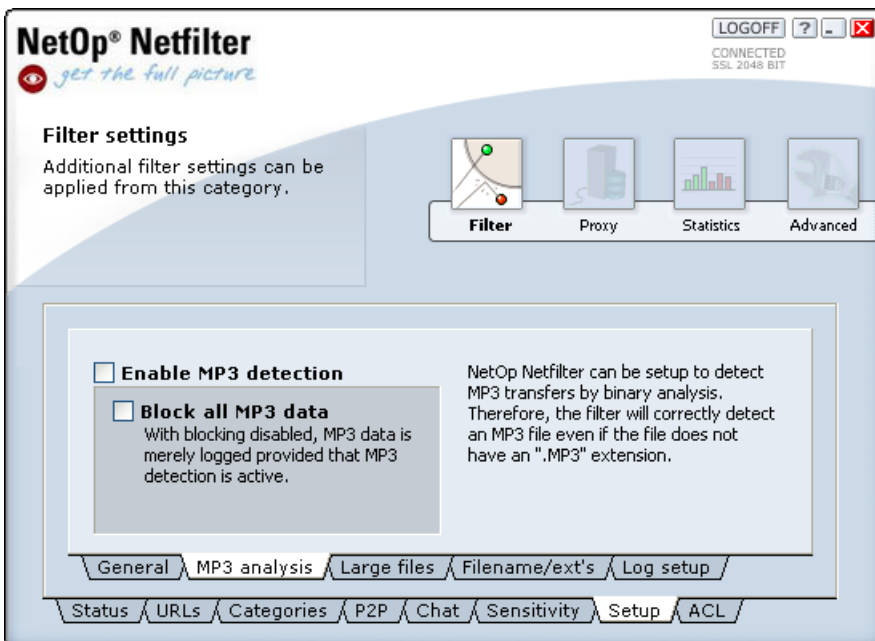
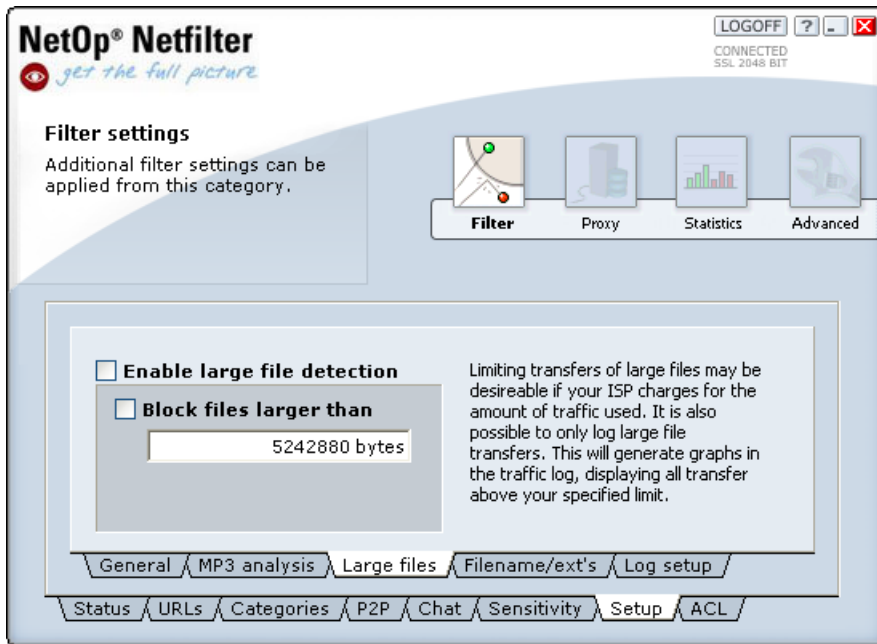


Figure 26: MP3 detection and blocking.

- 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.

See: [Filters MP3](#).

### 3.3.7.4 Large Files

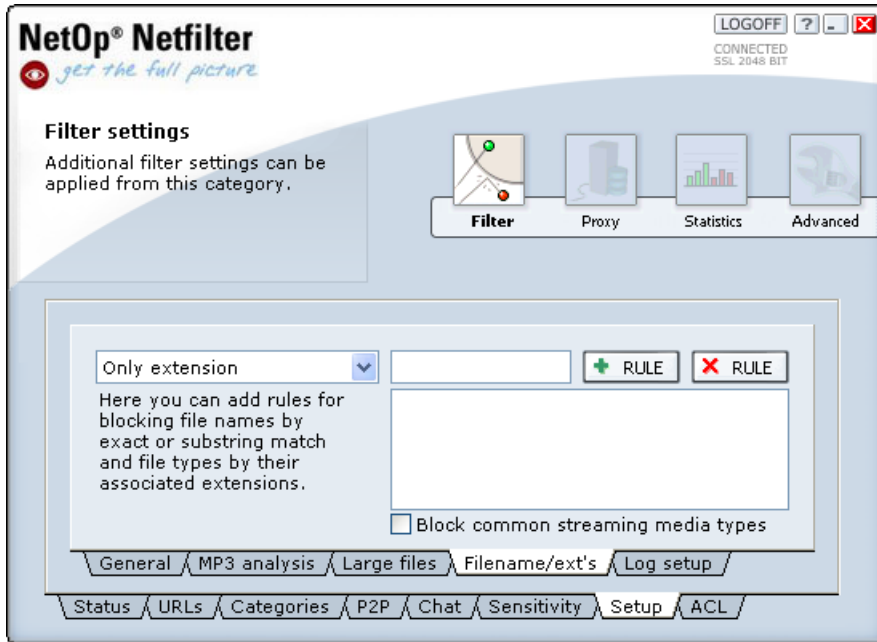


**Figure 27: Large file detection and blocking.**

- 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 MB.
- Block files larger than. Block for transfer of files larger than the specified limit and register transfer attempts in the log file.

See: [Filters Large Files](#).

### 3.3.7.5 Filename/ext's



**Figure 28: Blocking by name.**

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:

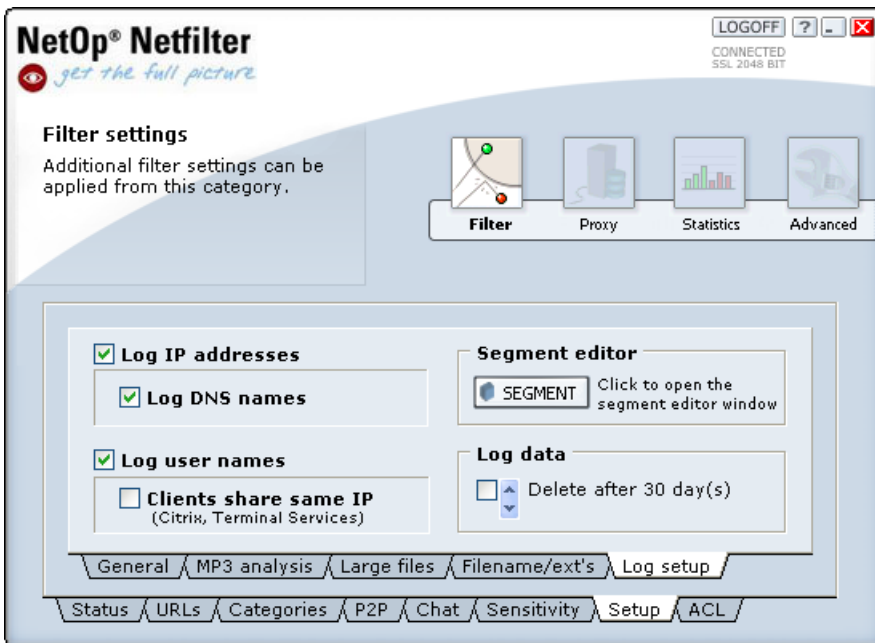
- Only extension. Enter extension, for instance "exe" or "zip", in the text field and press +RULE to add the extension to the list. Now, all files with the specified extension will be blocked.
- Exact filename. To block files with a specific name, enter the filename, e.g. "foo.exe", in the text field. 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.

See: [Filters Filename/exts.](#)

### 3.3.7.6 Log Setup

On the page Log setup it is possible to choose what should be logged about the user along with the addresses of visited sites. The default setting is to log only IP. If DNS is used on the network, the DNS addresses of the clients may also be logged.



**Figure 29: Logging of addresses and user names.**

If logging of user names is activated, the number of blocked and granted pages as well as the bandwidth consumption will be logged for each user rather than for each IP. It will also be logged which user (or users) that was logged in on the computer that was used to visit a web page. In the list of pages that has been visited using the client command "View page unblocked", it will be possible to see the name of the user who did this. Do not activate logging of user names unless [ECLIENT.EXE](#) is running on all clients.

**Note:** Logging of user names can only be used if ECLIENT.EXE is running on the clients. It is important that logging of user names is not activated before ECLIENT.EXE is running on all clients.

Log user names and Clients share same IP must be checked if several users are sharing the same IP address and ECLIENT.EXE must be running with the parameter [/sharedip](#). Several users are sharing the same IP address if Citrix or Terminal Services is used or if there is another [Proxy server](#) between the users and NetOp Netfilter.

**Note:** Correct logging of the traffic when the users are sharing an IP address requires that all users are using Internet Explorer as browser.

It is possible to automatically delete log data after a number of days, for instance to limit the consumption of disk space. To make use of this, Delete after N day(s) must be checked. The number of days are changed using the arrows.

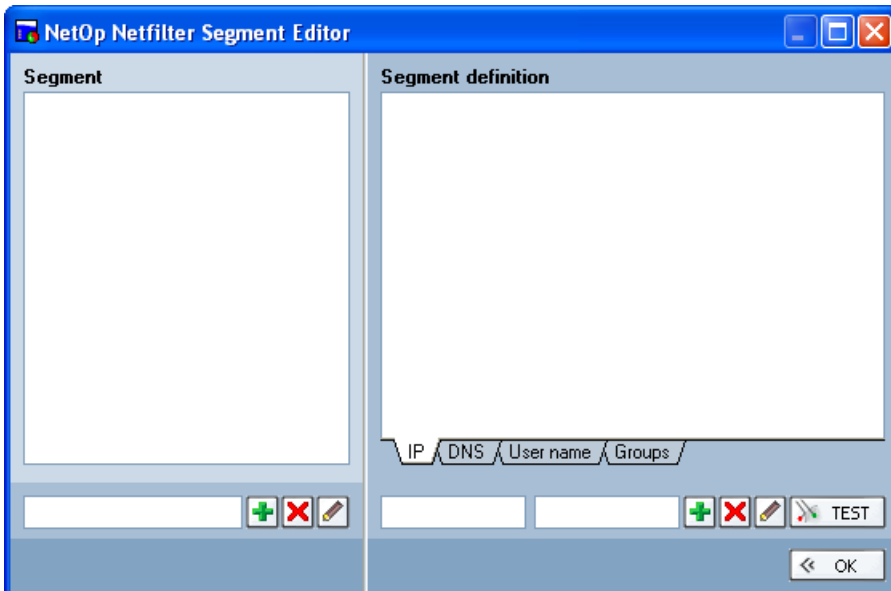
The button [SEGMENT](#) opens a window, where the division of the log into segment may be edited. This is described in the following section.

See: [Segments](#) and [Filters Log Setup](#).

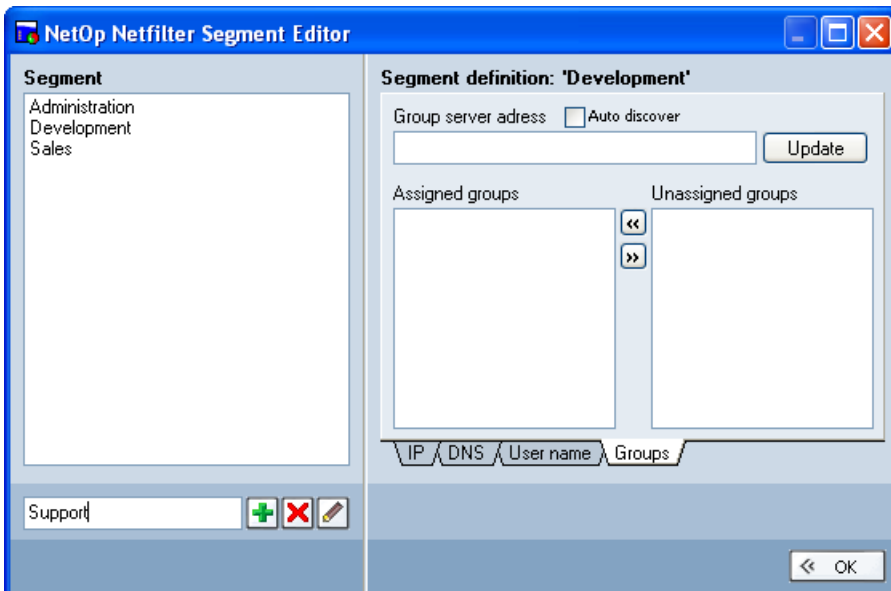
### 3.3.7.6.1 Segments

It is possible to perform a division of the log into [segments](#), such that a separate log is produced for each of these segments. The segments could for instance be departments in the organization. Each segment is defined by IP addresses, DNS suffixes, user names, and groups.

The division into segments is only effective from the time it is done, i.e. it is not possible to make a division of the existing log.



**Figure 30: Segments.**



**Figure 31: Groups.**

To the left in the window, shown in Figure 30, a list of segments is seen. When a segment is selected in this list, it can be seen to the right which IP addresses, DNS addresses, user names, and groups that will be logged under this segment.

To define a [new segment](#), the following must be done:


- Enter a name for the segment under the segment list and click + to create the segment.
- Under the IP tab, IP addresses of the computers which are to be logged under the segment may be entered. To add an interval of IP addresses, the first and last IP address of the interval is entered in the two fields. If just a single IP address is to be added, this is entered in the first field. Click + to add the address or interval to the segment.
- Under the DNS tab, DNS suffixes for the computers which are to be logged under the segment may be entered. Enter the suffix in the field and click + to add it. All computers which have a DNS name with the specified suffix will now be logged under the segment. The specified DNS suffixes will only be effective if logging of DNS names is activated (see [Log Setup](#)).


- Under the User name tab, names may be entered for the users that must be logged under the segment. Enter the name in the field and press + to add it. The specified user names will only be effective if user [name logging](#) is active.
- Under the Groups tab, which can be seen in Figure 31, groups whose members must be logged under the segment can be chosen. Choose the group in the list to the right and click on << to add it. The group may be removed from the segment using >>.

The list of groups is retrieved from a domain controller. If Auto discover is checked, Netfilter will try to locate a domain controller, otherwise the address of the domain controller must be specified under Group server address. If a domain controller is specified and Auto discover is checked, the specified domain controller will be used if it is available, otherwise Netfilter will attempt to locate another domain controller. Therefore, it is recommended that Auto discover is enabled even though an address has been specified.

Overlap between segments is allowed. For instance, the same user name may be added to several segments.

If a log for a particular user is desired, a segment may be created which contains only this user.

To [modify or delete](#) an IP interval, a DNS suffix, or a user name from the definition of a segment, the particular element is selected in the list. The element may now be deleted by clicking on X or modified by entering the new value and clicking on .

To rename a segment, it is selected in the list and the new name is entered. Then click on .

To delete a segment, select it in the list and click on X.

Under the [Test segment](#) tab, it is possible to see which segments an IP address, a DNS address, or a user name is logged under. Enter the address or name, choose which type of data it is, and click on TEST. The segments that the address or name will be logged under are now marked in the segment list.

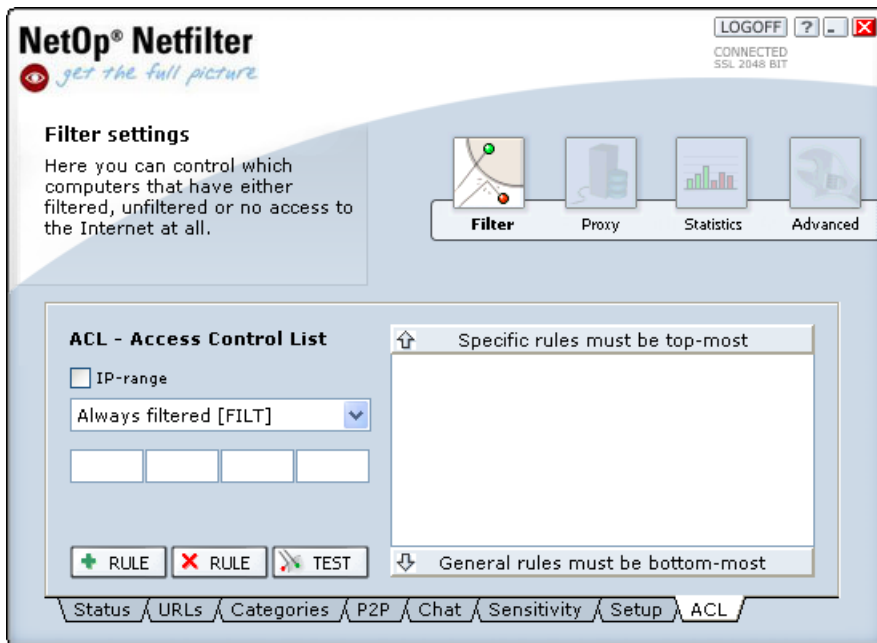
### 3.3.8 A C L

The tab ACL makes it possible to control which computers that have access to the Internet, and which sort of access the computers are to have. This is controlled with an [Access Control List](#) as shown in [Figure 32](#). It is possible to specify the [IP address](#) of a computer or an [IP range](#) for several computers, and choose which sort of filtering that must be used for the chosen computers. It is possible to choose between three types of filtering:

Always filtered	Always filter the traffic for the specified IP addresses.
Unfiltered	Never filter the traffic for the specified IP addresses.
<a href="#">Denied access</a>	Deny the specified IP addresses access to the Internet.

With these three types of filtering, it is possible to control the network in a very precise manner. For instance, in a company the accounting department may have one range of IP addresses and the development department may have another. Using ACL it is then possible to filter all computers in the accounting department but at the same time allow the computers in the development department to have unfiltered access, simply by adding two rules. If part of the company is to be denied access to the Internet, this can be done using the *Denied access* rule.

To add a single IP address, it is entered and the +RULE button is pressed. If you wish to add an IP range, this is done by checking the box IP range. It is now possible to specify two IP addresses. For instance, if you wish to filter computers from 10.0.0.1 to 10.0.0.50, 10.0.0.1 is entered in the upper field and 10.0.0.50 in the lower field.



**Figure 32: Configuration of access control list.**

To [remove a rule](#), it is selected with the mouse and the XRULE button is pressed.

To determine whether the rules have been correctly specified, it is possible with the [TEST](#) button to determine whether a single IP address is satisfied by one or more of the rules. This can be useful, if a very complex set of rules has been created, and there is doubt whether an IP is filtered as desired.

**Note:** It is important that the most specific rules are entered at the top. For instance, if filtering is wanted for all IP addresses except one in a range, this can be specified with a rule stating that filtering should not be used for that particular IP address, and then adding a rule below it that states that filtering must be used for the entire range.

See: [Access Control List](#) and [Troubleshooting](#)

## 3.4 Advanced Topic

A screenshot from this topic is shown in [Figure 35](#). Here, it is possible to set the more advanced properties, with regard to both *NetOp Netfilter Admin* and *NetOp Netfilter*. The three tabs under the *Advanced* topic make it possible to adjust properties that often can be left unchanged under normal circumstances.

See: [Netfilter Admin Settings](#), [Client Commands](#), [Block Pages](#), [Cache](#), [Time Schedule](#) and [Accounts & Privileges](#)

### 3.4.1 Netfilter Admin Settings

This tab, which is shown in [Figure 35](#), makes it possible to configure properties for NetOp 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.

It is possible to change the database used by NetOp Netfilter. Press the *Setup...* button to open a window that lets you enter address, user name, password, and database name. If you do not wish to use the database, leave these parameters unspecified. Data will then be logged to local log files on the Netfilter server.

Through [Accounts & Privileges](#) it is possible to create multiple user accounts that can be assigned different privileges.

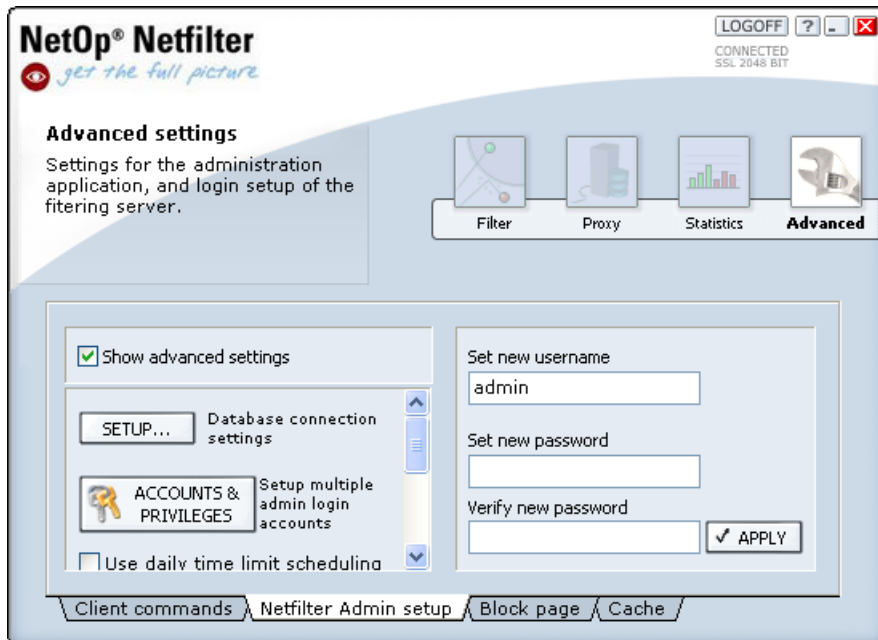
[Time scheduling](#) makes it possible to use different settings for the filter on different times of day and different weekdays. Check Use daily time limit scheduling to enable time scheduling and click on Schedule to set up the time schedule.

Click sounds on top buttons may be disabled for silent operation.

With Auto-Logout when placed in tray it is possible to choose whether the program must log of the filtering server when NetOp Netfilter Admin is minimized. This is to avoid forgetting to log of when leaving the computer.

Using [Test SSL](#) connection it can be chosen whether NetOp Netfilter Admin periodically should check if the encrypted connection between NetOp Netfilter Admin and NetOp Netfilter is open. Likewise, it is possible to choose how often NetOp Netfilter Admin must perform the check.

Username and password 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.



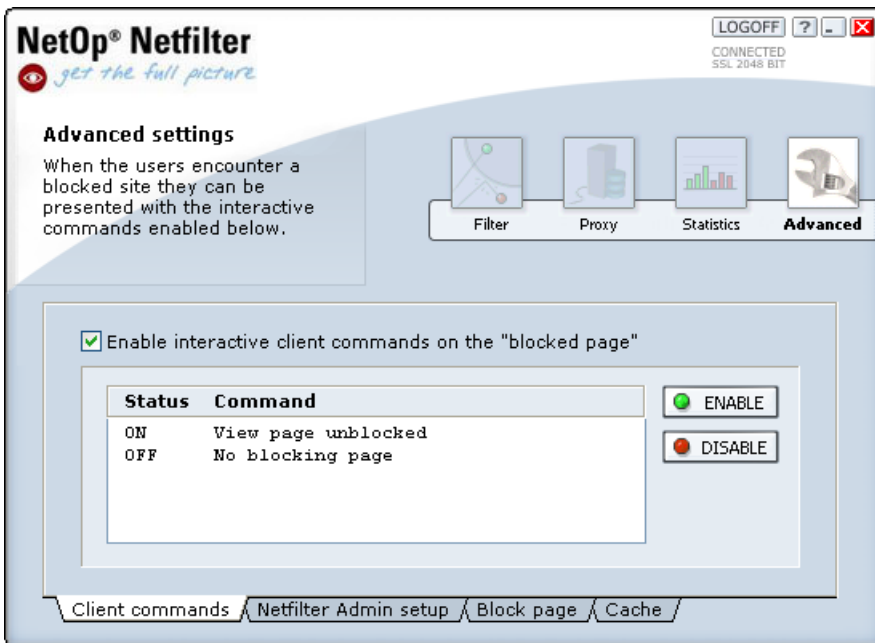
**Figure 35: Advanced settings for NetOp Netfilter Admin.**

See: [Troubleshooting](#)

### 3.4.2 Client Commands

The tab Client commands, shown in [Figure 36](#), 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.

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.



**Figure 36: Configuration of Client Commands.**

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.

When the command [No blocking page](#) is enabled, the pages that are visited are not blocked, but still logged.

See: [Troubleshooting](#)

### 3.4.3 Block Page

It can, as shown in [Figure 37](#), be changed which language that is used for the [block page](#). It is possible to choose between the listed languages. The block page is the page that is shown instead of the requested page, when NetOp Netfilter has found inappropriate material.

Furthermore, it is possible to replace the standard block page with a page based on a [HTML template](#).

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 and {%%} commands only replaces the tag occurrence

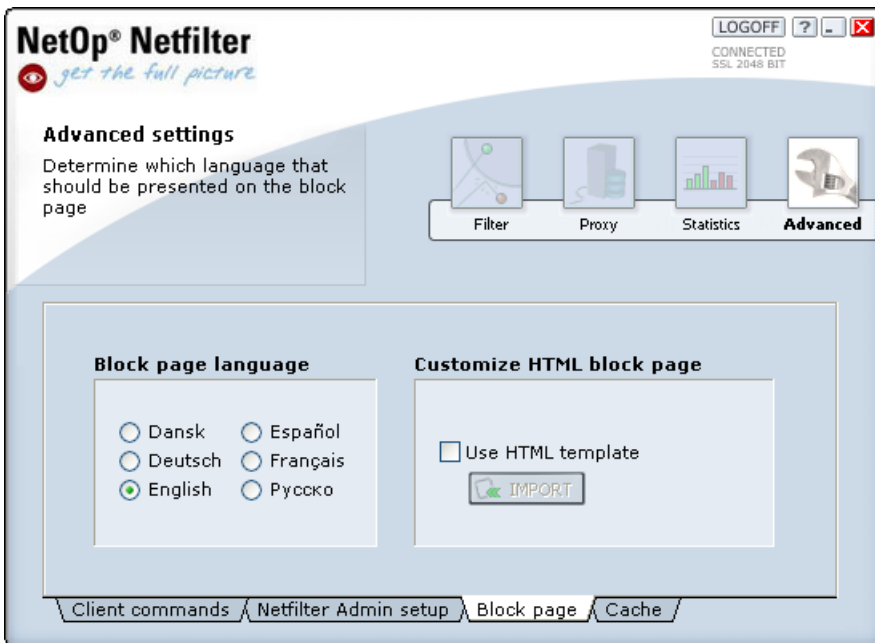


Figure 37: Configuration of block page.

See: [Troubleshooting](#)

### 3.4.4 Cache

NetOp Netfilter stores visited sites in a cache to improve speed when the pages are visited again.

To delete the contents of this cache: Select *Advanced Topic > Cache* and click *Reset*.

The numbers above the Reset button specifies the memory and disk space used for the cache.

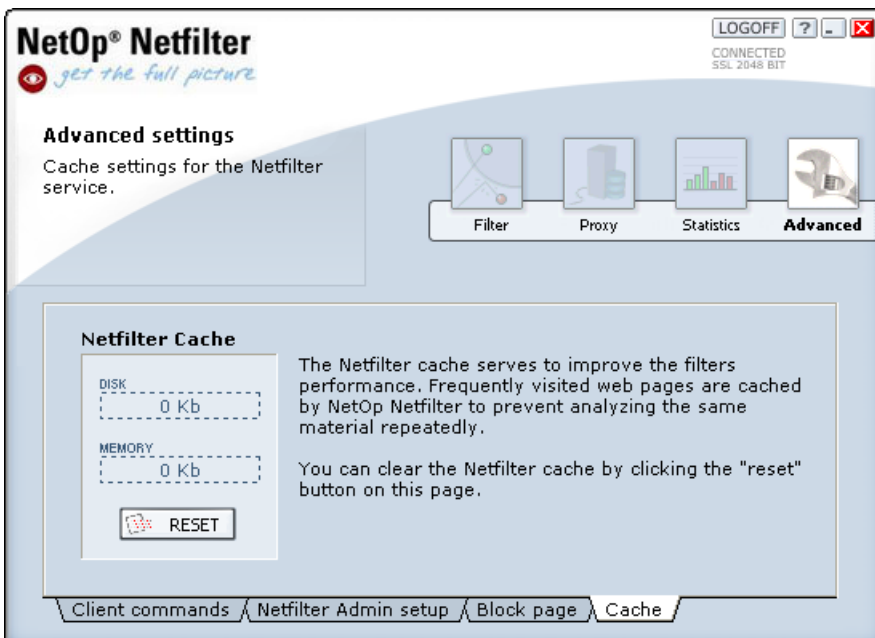
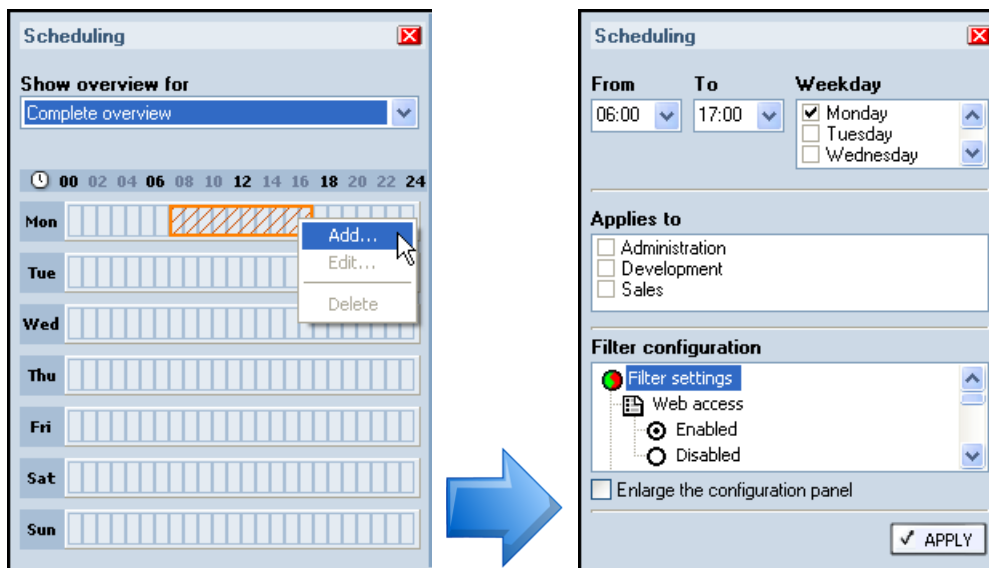


Figure 38: Cache.

See: [Troubleshooting](#)

### 3.4.5 Time Schedule

NetOp Netfilter allows you to vary some of the settings according to a [time schedule](#). These settings include whether a particular segment has access to the Internet, whether filtering is activated, and, if it is, what to block.



**Figure 39: Time schedule.**

To activate the use of a time schedule, check *Use time schedule* on the [Netfilter Admin setup](#) page under *Advanced*. Press the *SCHEDULE* button to edit the schedule.

When the time schedule is empty, the settings specified in the main window (as described in the previous sections) will be used. When settings have been specified for a block in the time schedule, these will override the settings specified in the main window.

Settings for a block in the time schedule can be added by clicking on the time slot for the start of the period and then, while keeping the mouse button pressed down, dragging to mark the desired period. When the period has been marked, right-click on the marked area and select *Add...* The contents of the window then changes to the settings panel shown to the right in [Figure 39](#).

In the settings panel, you can adjust the start and end of the period and choose which days of the week the settings you are specifying should be applied. You can also choose which segments these settings should be used for, i.e. different segments may have different settings for the same period of time.

The settings for the period you have selected are edited in the list at the bottom of the window. Refer to the previous sections for more information on these settings.

When you have specified which settings that must be used, which segments they must be used for, and when they must be used, press *APPLY*. This will bring you back to the time schedule, where you can add new blocks, modify settings for existing blocks, and delete blocks.

To modify the settings for a block, choose *Edit...* in the menu that appears when you right-click on the block. To delete a block from the time schedule, choose *Delete* in the menu.

If you wish to see how the schedule is for a particular segment, select that segment in the drop-down box at the top of the window.

To close the time schedule window, press the X button in the upper right corner of the window.

See: [Troubleshooting](#)

### 3.4.6 Accounts & Privileges

It is possible to create several user accounts and assign different privileges to different groups of users of Netfilter Admin.

User accounts are managed from the window shown in [Figure 40](#). In the upper part of the window, a list of group is shown. In the lower part, it is shown which group each user belongs to.

To create a new group, press *Add...* This will bring up a new window where name, description, and privileges for the group are chosen, see [Figure 41](#). The same window can later be opened by selecting the group and choosing *Properties*. Groups to which no users are assigned can be removed by pressing *Remove*.

A [group](#) can be assigned the privilege needed to modify the [Always block list](#) and the [Always grant list](#) or the privilege of unrestricted access to all settings.

A new [user](#) may be added with the button *Add...* below the list of user accounts. In the window that is shown, name, password, group membership etc. is chosen, see [Figure 42](#) and [Figure 43](#). If the account automatically must expire after some time, check *The account expires* and enter the date and time for expiry. As for groups, the properties for the user may be shown with *Properties* and the user may be removed with *Delete*.

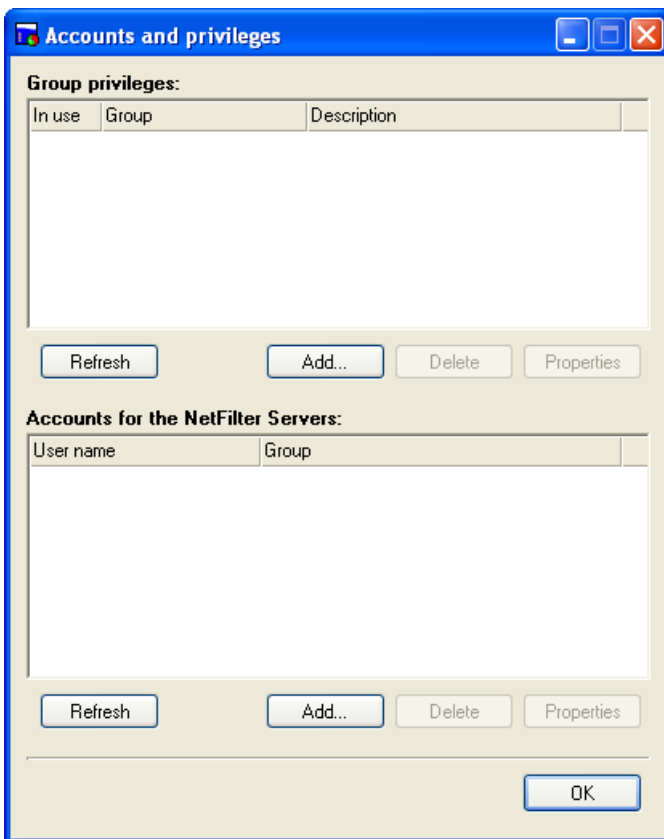


Figure 40: Account & Privileges.

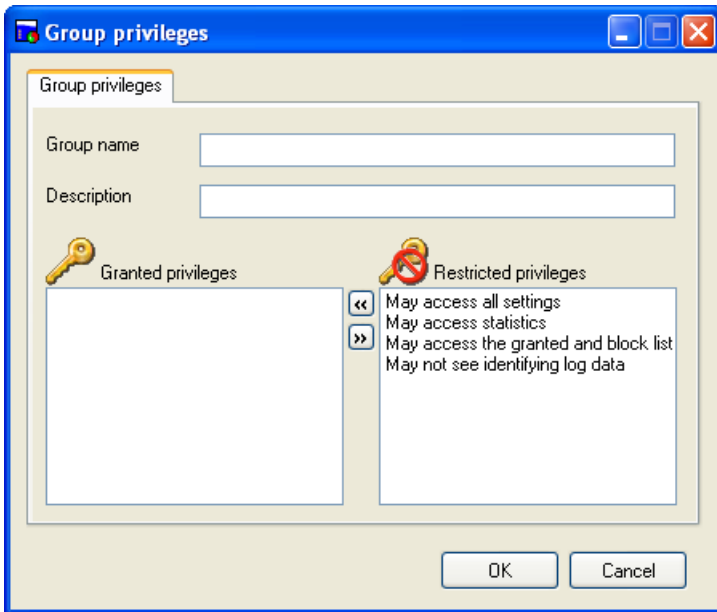


Figure 41: Properties for group.

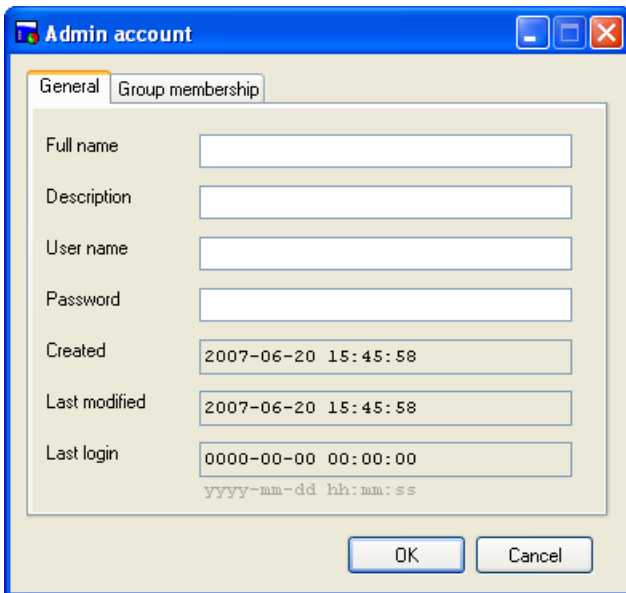


Figure 42: Properties for user.

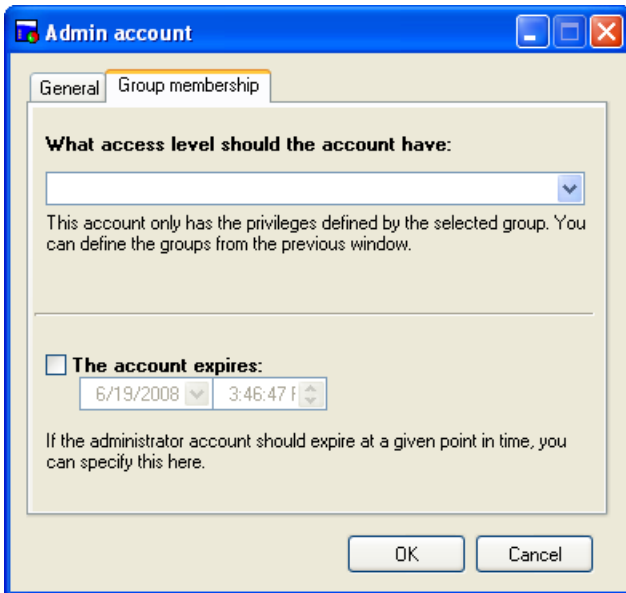


Figure 43: Properties for user.

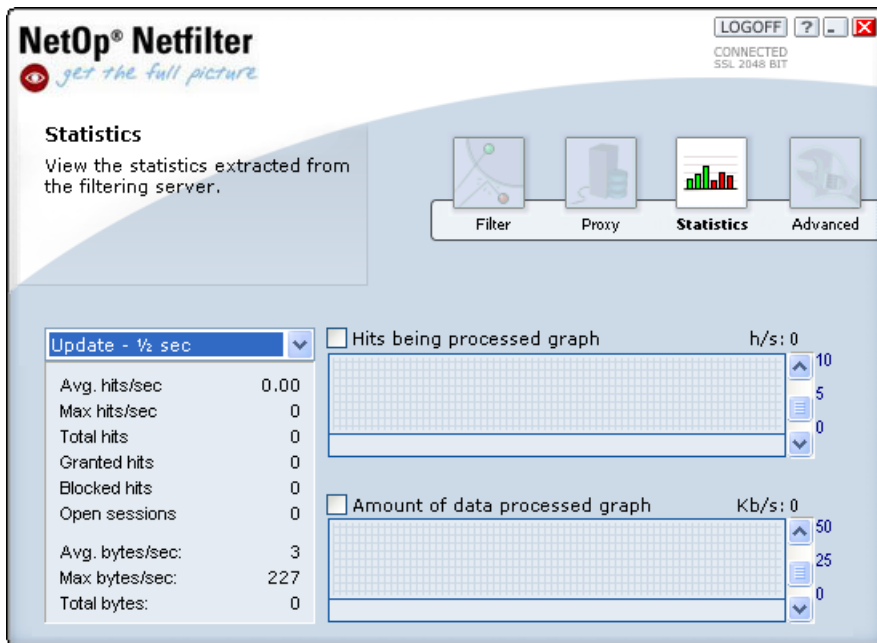
See: [Troubleshooting](#)

### 3.5 Statistics Topic

As it can be seen in the column at the left of the screenshot in [Figure 34](#), it is possible to see various information regarding the filter. These are described below. All the information in this column is measured over the period from last restart until now.

Avg. hits/sec	The average number of hits pr. second. A hit is a request for an Internet page.
Max. hits/sec	The maximal number of hits pr. second.
Total hits	The total number of requests.
Granted hits	The total number of requests that the filter has granted.
Blocked hits	The total number of requests that the filter has blocked.
Open sessions	The number of sessions (client connections) that are active in NetOp Netfilter right now.
Avg. bytes/sec	The average amount of data that are directed through NetOp Netfilter pr. second.
Max. bytes/sec	The maximal amount of data that has been directed through NetOp Netfilter in a single second.
Total bytes	The total amount of data which has been directed through the filter since last restart.

The bytes unit will change to Kb and then Mb as the amount of data grows.



**Figure 34: Statistics for NetOp Netfilter.**

See: [Graphs](#) and [Troubleshooting](#)

### 3.5.1 Graphs

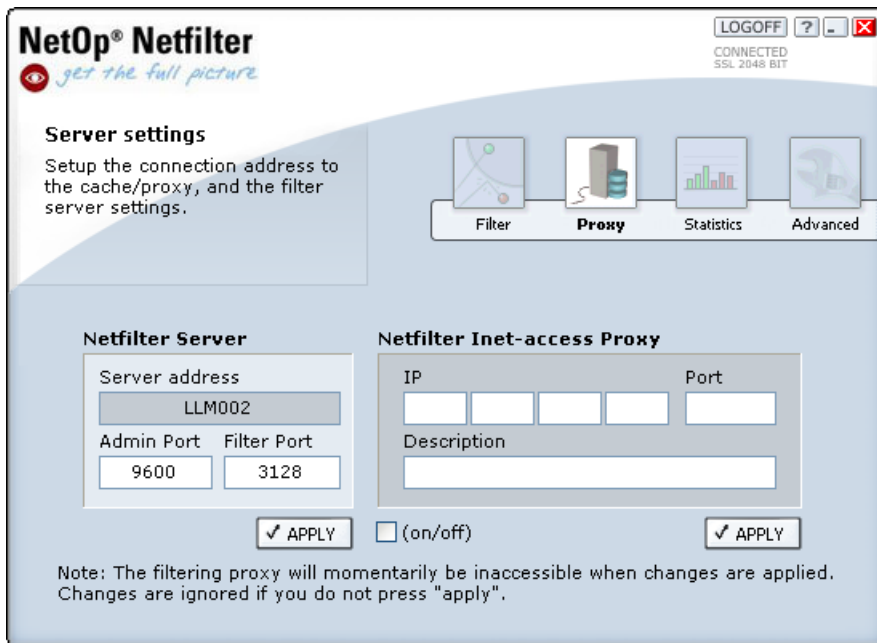
It is possible to monitor how large the load on NetOp Netfilter is. This is done by checking *Hits being processed* graph, *Amount of data processed* graph, or both. Hereby, it is possible to get an instant measure of the load on the server. *Hits being processed* graph shows how many hits pr. second that are directed through NetOp Netfilter in the moment, the graph is read, and *Amount of data processed* graph shows the total amount of data that is directed through NetOp Netfilter.

Both graphs are updated with the same interval as the information in the left column. It is possible to set the update frequency, see [Figure 34](#). The range of each graph window can be set using the slider to the right.

See: [Statistics Topic](#)

## 3.6 The Proxy Topic

This topic makes it possible to configure which ports NetOp Netfilter operates on, as well as whether the traffic from NetOp Netfilter should be directed through an external proxy.



**Figure 33: Configuration of NetOp [Netfilter port](#) numbers and external proxy.,**

See: [Proxy](#), [Netfilter Proxy](#) and [Netfilter Inet-access Proxy](#)

### 3.6.1 Netfilter Proxy

Here, it is possible to configure which port that is to be used by browsers for Internet access through NetOp 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 NetOp 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 NetOp Netfilter that is used for communication with NetOp 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 NetOp Netfilter Admin, the new port must be entered instead, as described in [Login](#). The modifications of the port settings will not be activated until the APPLY button has been pressed.

**Note:** NetOp Netfilter for a short period of time will be inactive while it adapts to the changes.

**Note:** If the port 9600 already is taken on the computer that NetOp Netfilter is running on, the port for NetOp Netfilter Admin can be changed by editing the text file *Data/ProxyAdminPort.cfg*, which is placed in the NetOp Netfilter folder on the filtering server. Only after that has been done is it possible to communicate with NetOp Netfilter through NetOp Netfilter Admin.

See: [Proxy](#), [The Proxy Topic](#), [Netfilter Inet-access Proxy](#) and [Troubleshooting](#)

### 3.6.2 Netfilter Inet-access Proxy

It is possible to connect NetOp Netfilter with an external [Proxy](#) server, as described in [Features](#). 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 NetOp 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 NetOp 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 NetOp Netfilter for a short period will be inactive while it adapts to the changes.

See: [Proxy](#), [The Proxy Topic](#), [Netfilter Proxy](#) and [Troubleshooting](#)

### 3.7 Troubleshooting

In this section, some of the problems that may arise when using NetOp Netfilter are described. If the suggested solutions below do not solve the problem, you may try restarting the filtering server.

#### **No Internet connection through NetOp Netfilter.**

First, determine whether there is connection to the Internet from the filtering server, that is, the computer that NetOp Netfilter is installed on. If there is no connection, try to re-establish the connection.

If there is connection to the Internet from the filtering server, the cause of the problem can be that the [Filter Port](#), which is used for communication between NetOp Netfilter and the clients, are being used by another program on the server. In this case, NetOp Netfilter will inform about the problem when the filtering server is restarted. The problem can be solved by either

- configuring NetOp Netfilter and the clients in the network to use another [Filter Port](#), or
- configuring (or uninstalling) the other program such that it will not use the same port as NetOp Netfilter.

#### **NetOp Netfilter Admin cannot establish connection to the NetOp Netfilter server.**

Determine whether another server is using the port, which is used for communication between the NetOp Netfilter server and NetOp 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 NetOp Netfilter by editing the text file *Data\ProxyAdminPort.cfg*, which is placed in the NetOp Netfilter folder on the filtering server. Alternatively, you can stop the other server, log on to the NetOp Netfilter server using NetOp 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 NetOp 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 NetOp Netfilter as proxy server. If not, configure the browser with the address and port for the NetOp 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 NetOp 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 NetOp 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 when the page is shown in Internet Explorer.**

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 *NetOp Netfilter.exe* have full access to the Internet. This setting may be changed in the administration program for Norton Internet Security. The setting for NetOp Netfilter should be *Permit All*.

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 NetOp 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 NetOp 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 NetOp 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 NetOp 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). NetOp 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 NetOp 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 NetOp Netfilter is used.

### **The Internet connection becomes very slow when logging of user names is activated.**

[ECLIENT.EXE](#) must be running on all clients before logging of user names is activated. If this is not the case, the Internet connection will become very slow for users that ECLIENT.EXE is not running for.

## **3.8 Blacklists**

Blacklists – lists of web sites that should be blocked – may be added as categories in Netfilter by copying them to Netfilter's "Blacklists" directory, which is located in the directory to which Netfilter was installed.

When the blacklists have been loaded by Netfilter (see [Loading the blacklists](#)), you need to enable them as described in [Filter Topic](#).

### **File format**

Blacklists are simply text files with one URL per line. For each blacklists, an .ini file supplying additional information needed by Netfilter must be created. We recommend giving the blacklist and the .ini file the same name, apart from the extension, e.g. "your\_blacklist.txt" and "your\_blacklist.ini".

The .ini file should look like this:

```
[Config]
blacklistfilename=your_blacklist.txt
```

```
displayname=Name of your blacklist
description=Description of your blacklist.
uniqueid=UID_YOURBLACKLIST
```

`blacklistfilename` is the name of the blacklist file.

`displayname` is the name that will be shown in Admin, Log Viewer, and on the block page.

`description` will be shown in Admin and should provide details about what kind of sites the blacklist contains.

`uniqueid` is an identifier that is used internally in Netfilter. You cannot have two blacklists with the same identifier, so this must be chosen with care. For instance, you could include your company name in the identifier to make it unique.

### Loading the blacklists

Netfilter will automatically load new blacklists at 2 AM. If you want to load them at another time, you can do this by restarting the Netfilter service manually. A blacklist will not become active until it has been fully loaded.

### Installing blacklists on multiple servers

Blacklists are assigned numeric IDs by Netfilter. If you install the same blacklists on multiple servers and are logging to a single database, these IDs must be identical. Netfilter stores the IDs in a file named `categoryids.ini` in the root of the Netfilter directory.

If you always install new blacklists in the same sequence on all servers, they should be assigned identical IDs.

However, we recommend adhering to the following procedure when installing blacklists on multiple servers:

1. Stop the Netfilter service on one of the servers.
2. Copy the blacklist files to this server and start the Netfilter service.
3. For each of the remaining servers, stop the Netfilter service, copy the blacklist files to the server, copy the `categoryids.ini` file from the *first server*, and restart the service.

You may choose not to install all blacklists on all servers, but the one that you copy the `categoryids.ini` from MUST have all blacklists installed.

## 4 Handling

The Help pages are all accessed from the Netfilter GUI.

Here, they are organized in terms of functionality.

<a href="#">Login</a>	<a href="#">Filter: Status</a>	<a href="#">Advanced: Client commands</a>
<a href="#">Proxy</a>	<a href="#">Filter: URL lists</a>	<a href="#">Advanced: Netfilter Admin settings</a>
<a href="#">Statistics</a>	<a href="#">Filter: Categories</a>	<a href="#">Advanced: Block page</a>
	<a href="#">Filter: P2P</a>	<a href="#">Advanced: Cache</a>
	<a href="#">Filter: Chat</a>	<a href="#">Advanced: Time schedule</a>
	<a href="#">Filter: Sensitivity</a>	<a href="#">Advanced: Accounts &amp; Privileges</a>
	<a href="#">Filter: Setup</a>	
	<a href="#">Filter: Network Setup</a>	
	<a href="#">Filter: Segments</a>	
	<a href="#">Filter: ACL</a>	

### 4.1 Login page

To administrate a Netfilter server, you must login first. All communication between the administration program Netfilter Admin and the Netfilter server is encrypted.

<b>Remote Server Address</b>	Here you should enter the IP address and Port of the Netfilter server you wish to administrate.
<b>Administrator username</b>	The default username is 'admin'. If you have <a href="#">modified your username</a> , you will need to supply the modified username instead.
<b>Administrator password</b>	The default password is 'admin'. This password must be <a href="#">changed</a> after the first login to prevent unauthorized access to the server.

### 4.2 Filters

NetOp Netfilter offers a wide variety of filter types to meet the changing needs of filtering. The following sections describe how filters are used and what to take into consideration.

See: [Status](#), [URLs](#), [Categories](#), [Peer-2-peer](#), [Chat](#), [Sensitivity](#), [Setup](#), [Network Setup](#), [Segments](#) and [Access Control List](#)

#### 4.2.1 Status

The [Status](#) page is shown after a successful login. It can also be displayed by pressing the status tab, accessible from the Filter configuration pages.

The page displays a number of status elements, described below. Furthermore, it is possible with the 'SEARCH LOG'-button to get detailed information about the traffic through the filter.

Version	This is the version number and release date of the Netfilter server.
Filtering server hostname and status	Here you can see the hostname of the Netfilter server, and an indication of its <a href="#">status</a> (either enabled or disabled). If the Netfilter server is disabled a red warning marker will be visible. By clicking this marker additional information will be displayed regarding how to bring the server back to its enabled state.

Internet Access Proxy IP and description	This is the IP address of the Internet Access Proxy used by the Netfilter server. Also, a textual description is provided for the Internet Access Proxy. If an Internet Access Proxy is not used, the text 'disabled' will be displayed instead.
Service started	This field indicates when the Netfilter server was originally started, and thus provides a measure for its uptime.
Bytes processed	The total number of bytes processed by the Netfilter server during its uptime.
Results	The total number of hits and the amount of these that has been blocked.

See: [Status](#) and [Statistics page](#).

See: [Filters](#), [URLs](#), [Categories](#), [Peer-2-peer](#), [Chat](#), [Sensitivity](#), [Setup](#), [Network Setup](#), [Segments](#) and [Access Control List](#)

## 4.2.2 URLs

### URL lists

URL's listed in 'Always grant list' will be shown to the clients without being analyzed. URL's listed in 'Always block list' will be blocked without actual data retrieval from the Internet and therefore also without any analysis. If an URL is specified in the blocked list, it is not possible to continue to the page from the block page, regardless of the settings for [client commands](#). The URL's in the blocked list will be blocked in this manner for any client, except clients that match possible [ACL rules](#) specifying that their Internet access should be unfiltered.

### Adding an URL

To add a new URL to a list, you simply enter the URL in the text field and then click Add URL.

### Removing an URL

To remove an URL from a list, first select the URL from the list by clicking it once with the left mouse button such that the URL becomes highlighted, then press the Del URL button.

See: [Filters](#), [Status](#), [Categories](#), [Peer-2-peer](#), [Chat](#), [Sensitivity](#), [Setup](#), [Network Setup](#), [Segments](#) and [Access Control List](#)

## 4.2.3 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 to the left. When a category is marked, a description of the category is shown to the right.

See: [Filters](#), [Status](#), [URLs](#), [Peer-2-peer](#), [Chat](#), [Sensitivity](#), [Setup](#), [Network Setup](#), [Segments](#) and [Access Control List](#)

## 4.2.4 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.

### Program list

In the list to the left, 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.

### **Adding a program**

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.

### **Removing a program**

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.

See: [Filters](#), [Status](#), [URLs](#), [Categories](#), [Chat](#), [Sensitivity](#), [Setup](#), [Network Setup](#), [Segments](#) and [Access Control List](#)

## **4.2.5 Chat**

### **Program list**

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.

### **Adding a program**

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.

**Note:** 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.

### Removing a program

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.

See: [Filters](#), [Status](#), [URLs](#), [Categories](#), [Peer-2-peer](#), [Sensitivity](#), [Setup](#), [Network Setup](#), [Segments](#) and [Access Control List](#)

## 4.2.6 Sensitivity

Using the slider on this page, you can adjust the filtering sensitivity to suit your preferences. It is possible to choose between three settings for sensitivity, Low, Normal, and High.

<b>Low</b>	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.
<b>Normal</b>	Normal is the standard setting for the filter and is recommended for normal use.
<b>High</b>	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.

See: [Filters](#), [Status](#), [URLs](#), [Categories](#), [Peer-2-peer](#), [Chat](#), [Setup](#), [Network Setup](#), [Segments](#) and [Access Control List](#)

## 4.2.7 Setup

From this configuration page, you can enable or disable certain filter features.

<u>General</u>	
Disable filter completely	Toggles the Netfilter servers role. When the filter is disabled, the proxy simply provides its clients with an unfiltered Internet access.
Config backup	This makes it possible to save a copy of the configuration in a local file and later load it to restore the configuration.
Network setup	Makes it possible to send the current setup to a number of other servers over the network.
<u>MP3 analysis</u>	

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.
<b>Large files</b>	
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.
<b>Filename/ext's</b>	
Under the tab Filename/ext's, it is possible to configure blocking using rules based on the filename.	
Block common streaming media types	If Block common streaming media types is checked, rules for the most common types of streaming media are added.
Adding rules	It is possible to add rules in three different categories: <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> </ul>
Removing rules	A rule may be deleted by selecting the rule in the list and pressing XRULE.
<b>Log setup</b>	
Here, it is possible to choose what should be logged about the user along with the addresses of visited sites	
Log IP addresses	When this is checked, the IP address of the user is logged when a page is visited.
Log DNS names	If DNS is used on the network, the DNS addresses of the clients may be logged by checking this option. If DNS is not used, this feature should not be active.
Log user names	If logging of user names is activated, it will also be logged which user (or users) that was logged in on the computer that was used to visit a web

	page. In the list of pages that has been visited using the client command 'View page unblocked', it will be possible to see the name of the user who did this.
Clients share same IP	'Clients share same IP' must be checked if several users are sharing the same IP address and user name logging is active. <a href="#">ECLIENT.EXE</a> must be running with the parameter <a href="#">/sharedip</a> as described in the manual. Several users are sharing the same IP address if Citrix or Terminal Services is used or if there is another proxy server between the users and NetOp Netfilter. Note that correct logging of the traffic when the users are sharing an IP address requires that all users are using Internet Explorer as browser.

See: [Filters](#), [Status](#), [URLs](#), [Categories](#), [Peer-2-peer](#), [Chat](#), [Sensitivity](#), [Network Setup](#), [Segments](#) and [Access Control List](#)

## 4.2.8 Network Setup

With [Network Setup](#) it is possible to manage a number of Netfilter servers at the same time. It is done by customizing the settings on one server and then transferring the settings of this server to the rest. The servers that the settings must be sent to are added to the list. Then 'Apply' is pressed to send the settings to the specified servers.

Proxy settings are only sent to the other server if 'Also copy proxy settings' is checked.

See: [Filters](#), [Status](#), [URLs](#), [Categories](#), [Peer-2-peer](#), [Chat](#), [Sensitivity](#), [Setup](#), [Segments](#) and [Access Control List](#)

## 4.2.9 Segments

It is possible to perform a division of the log into [segments](#), such that a separate log is produced for each of these segments. The segments could for instance be departments in the organization. Each segment is defined by IP addresses, DNS suffixes, and user names.

The division into segments is only effective from the time it is done, i.e. it is not possible to make a division of the existing log.

To the left in the window, a list of segments is seen. When a segment is selected in this list, it can be seen to the right which IP addresses, DNS addresses, and user names that will be logged under this segment.

It is possible to have the segment definitions shown in a larger window.

See: Figures [30](#) and [31](#)

### Adding segments


To define a new segment, the following must be done:


- Enter a name for the segment under the segment list and click + to create the segment.
- Under the IP tab, IP addresses of the computers which are to be logged under the segment may be entered. To add an interval of IP addresses, the first and last IP address of the interval is entered in the two fields. If just a single IP address is to be added, this is entered in the first field. Click + to add the address or interval to the segment.
- Under the DNS tab, DNS suffixes for the computers which are to be logged under the segment may be entered. Enter the suffix in the field and click + to add it. All computers which have a DNS name with the specified suffix will now be logged under the segment. The specified DNS suffixes will only be effective if logging of DNS names is activate.
- Under the User name tab, names may be entered for the users that must be logged under the segment. Enter the name in the field and press + to add it. The specified user names will only be effective if user name logging is active.

Overlap between segments is allowed. For instance, the same user name may be added to several segments.

If a log for a particular user is desired, a segment may be created which contains only this user.

**Modifying and deleting segments**

To modify or delete an IP interval, a DNS suffix, or a user name from the definition of a segment, the particular element is selected in the list. The element may now be deleted by clicking on X or modified by entering the new value and clicking on .

To rename a segment, it is selected in the list and the new name is entered. Then click on .

To delete a segment, select it in the list and click on X.

**Testing segment definitions**

Under the Test segment tab, it is possible to see which segments an IP address, a DNS address, or a user name is logged under. Enter the address or name, choose which type of data it is, and click on TEST. The segments that the address or name will be logged under are now marked in the segment list.

See: [Setup Segments](#).

See: [Filters](#), [Status](#), [URLs](#), [Categories](#), [Peer-2-peer](#), [Chat](#), [Sensitivity](#), [Setup](#), [Network Setup](#) and [Access Control List](#)

**4.2.10 Access Control List**

Here you can set up simple rules to control the access privileges on your network. Clients can either have normal access to the Internet (i.e. unfiltered), filtered access, or no access at all. These modes are denoted as NORM, FILT, and DENY respectively. The set of rules is referred to as an [Access Control List](#) or [ACL](#).

<b>Identification of clients</b>	An ACL rule is specified using the IP addresses of the clients that are to be affected by the rule.
<b>Position of ACL rules</b>	The ACL rules currently used by the Netfilter server is displayed in the rightmost listbox. An ACL rule has the form 'rule ip' or 'rule ip-ip', allowing either rules spanning over single IPs or IP-ranges. Specific rules must be topmost, and general rules bottommost. This is important, as the first rule from the top that fits an inbound IP will be followed. That is, if a client with IP 10.2.3.4 requests a homepage from the Netfilter server and the rules listed are 'DENY 10.0.0.0-10.255.255.255' and then 'FILT 10.2.3.4', the request will be denied as the first rule, which is more general than the last rule, contains the clients IP address. Had the rules been swapped, such that they would have been listed as 'FILT 10.2.3.4' and then 'DENY 10.0.0.0-10.255.255.255', the clients request would have been processed as filtered. Rules can be positioned by clicking the two buttons placed above and below the ACL listbox.
<b>Adding a single-IP rule</b>	Select the mode as being 'single IP' (the checkbox 'IP-range' must be unchecked). Select the desired rule, unfiltered access (NORM), filtered (FILT), or <a href="#">Denied access</a> (DENY). Then enter the IP address of the client, and press '+RULE'. Finally, place the rule at the desired position in the list. Single IP rules are the most specific and should therefore be placed topmost in the list.
<b>Adding an IP-range rule</b>	Select the mode as being 'IP-range' (the checkbox must be checked). Select the desired rule, unfiltered access (NORM), filtered (FILT), or

	<a href="#">Denied access</a> (DENY). Then enter the first IP address in the upper IP input field and the last address in the lower IP input field and press '+RULE'. Finally, move the rule according to its granularity. Ranged IP rules are considered as general rules and should therefore be placed below any single-IP rules.
<b>Deleting an ACL rule</b>	Simply select a rule by left-clicking on it in the list. Then press the 'XRULE' button or the DEL button on your keyboard.
<b>Testing the ACL rule list</b>	To check if the rules behave as intended you can click the 'TEST' button. This displays a new input panel on the ACL page. From this panel, you can enter any IP address you wish. When you press the 'TEST IP' button you will immediately see the verdict for that given IP according to the current ACL rules.

See: [Filters](#), [Status](#), [URLs](#), [Categories](#), [Peer-2-peer](#), [Chat](#), [Sensitivity](#), [Setup](#), [Network Setup](#) and [Segments](#)

### 4.3 Proxy

This settings page allows you to view and modify the server connections. The Netfilter server can either access the Internet directly, or through an Internet Access Proxy (e.g. Squid).

**Note:** Changes in these settings are not applied to the server until the 'APPLY' button is actually pressed.

Netfilter Proxy settings	
Server address	This is a read-only field. It indicates the server name reported by the Netfilter server.
Admin Port	From here you can set the Netfilter administration server port. This port is used to exchange configuration and statistical data between the Netfilter server and a Netfilter Admin administration program. The default value for this port is 9600. You may need to change it if it is used by another program on the server. <ul style="list-style-type: none"> <li>Valid value is an integer number between 0 and 65535.</li> </ul>
Filter Port	This port is used by the clients for Internet access through the Netfilter server. The default value for this port is 3128. You may need to change it if it is used by another program on the server. <ul style="list-style-type: none"> <li>Valid value is an integer number between 0 and 65535.</li> </ul>
Netfilter Inet-access Proxy settings	
On/Off toggle	Turning the Netfilter Internet Access Proxy on will result in all Internet traffic being directed through an external proxy server. This may facilitate the integration of NetOp Netfilter in an existing network already using a proxy server. To use this functionality, a proxy server must be running and be accessible to the Netfilter server.
IP	The IP address of the machine running the proxy server. <ul style="list-style-type: none"> <li>Valid value is four integer values between 0 and 255.</li> </ul>
Port	The port on which the proxy server is running. <ul style="list-style-type: none"> <li>Valid value is an integer number between 0 and 65535.</li> </ul>
Description	Any textual description of the proxy server you would like to enter, e.g. the hostname and proxy model.

- Valid value is any text string.

## 4.4 Statistics

While the Netfilter Admin program is connected to the Netfilter server, it is continuously provided with live statistical data from the server. The [statistics page](#) allows you to inspect these data both numerically and graphically.

### Update frequency

The update frequency can be one of the following values: Frequently, ½ sec., 1 sec., and 5 sec. Selecting among these changes the delay between each new update from the Netfilter server.

### The numerical data

Avg. hits/sec	Number of hits processed per second.
Max hits/sec	Number of hits recorded to have been processed per second.
Total hits	Total number of hits that the server has processed for all its clients .
Granted hits	Number of hits that have been granted by the filter, and therefore have been displayed by the clients.
Blocked hits	Number of hits that have been blocked and therefore have been withheld by the Netfilter server.
Open sessions	Number of currently active client requests.
Avg. bytes/sec	Average number of bytes processed each second on the server.
Max bytes/sec	Recorded maximum number of bytes processed per second on the server.
Total bytes	Total number of bytes the server has processed.

**Note:** The unit 'bytes' will be changed automatically to Kb and then Mb as the numbers grow.

### The hits/sec graph

This graph displays, when activated, the number of hits (or requests) that the server currently processes per second. This is displayed with the gray graph line. If the graph is blank, no data is processed. The average number of hits processed per second is also displayed with a solid gray background graph.

### The bytes/sec graph

This graph displays, when activated, the number of bytes that the server currently processes per second. This is displayed with the gray graph line. If the graph is blank, no data is processed. The average number of bytes processed per second is also displayed with a solid gray background graph.

See: [Status](#).

## 4.5 Advanced Settings

The Advanced settings are accessed by clicking the Advanced button.

See: [Advanced Topic](#), [Interactive client commands](#), [Netfilter Admin Settings](#), [Block Page](#), [Cache](#), [Time Schedule](#) and [Accounts & Privileges](#)

### 4.5.1 Interactive client commands

The interactive [client commands](#) are provided by the Netfilter server. Depending on the version of the server the commands available may vary. At the time of writing, only one command is available.

<b>Enabling and disabling client commands</b>	<p>To use client commands, check the checkbox 'Enable interactive client commands on the blocked page'.</p> <p>To enable a particular client command, thus allowing clients to use it on the 'blocked page', simply select the command from the list and press the 'ENABLE' button.</p> <p>Similarly, to disable a command, select it and click the 'DISABLE' button.</p>
<b>'View page unblocked'</b>	<p>When enabled, this command will allow the users to continue to the page that was blocked by pressing a button on the 'blocked page'. A text on the 'blocked page' will warn the user that access to the material will be registered in the log.</p>
<b>'No blocking page'</b>	<p>When this command is enabled, the pages that are visited are not blocked, but still logged.</p>

## 4.5.2 Netfilter Admin settings

On this configuration page you can change the settings specific to the administration program.

<b>Show advanced settings</b>	<p>If this checkbox is checked, the more advanced settings are shown. Usually, it is not necessary to change these settings.</p>
<b>Database connection settings</b>	<p>It is possible to change the database used by NetOp Netfilter. Press the 'Setup' button to open a window that lets you enter address, user name, password, and database name. If you do not wish to use the database, leave these parameters unspecified. Data will then be logged to local log files on the Netfilter server.</p>
<b>Use daily time limit scheduling</b>	<p>Time scheduling makes it possible to use different settings for the filter on different times of day and different weekdays. Check Use daily time limit scheduling to enable time scheduling and click on Schedule to set up the time schedule.</p>
<b>Click sounds on top buttons</b>	<p>Click sounds on top buttons may be disabled for silent operation.</p>
<b>Test SSL connection</b>	<p>If you experience an unreliable Internet connection to the server, i.e. you are not using an always on connection (modem or similar), you could benefit from enabling this feature. When the test is enabled, the administration program periodically sends out 'Are-You-Alive' messages to the server. If a reply is not received, you will be informed that the connection has been disrupted. Any recently modified settings may have been lost because of the lost connection.</p>
	<p>The test interval can be either frequent or rarely. A frequent interval may be of use if you are a modem user. The less intense setting may be useful if you are using a faster connection and are experiencing occasional drop-outs.</p>
<b>Auto-logout</b>	<p>You can choose to make the administration program logout automatically when you minimize the application to the tray. To do so, simply enable this feature.</p>
<b>Modifying your username and</b>	<p>If you wish to modify your username and/or password, you can enter the new information in the text fields. When you press the 'OK'</p>

<b>password</b>	button, you will be informed of whether or not the operation was a success. Modifying this information also changes the encryption between the administration program and the server.
-----------------	---

**Warning:** If you loose your login information you will be unable to establish an administrative connection to the server.

See: [Netfilter Admin Settings](#).

### 4.5.3 Block page

#### Block page language

The [block page](#) is available in several languages. Choose the language appropriate for your users from the list.

#### Customize HTML block page

The standard block page may be replaced with a customized page based on a HTML template by importing the template with 'Import template...' and checking 'Use HTML template'. The template must be a HTML page containing one or more of the following tags:

HTML Tag	Description		
[%filter-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.		
[%filter-message %]	The line with this tag will be replaced with a message stating that the page has been blocked.		
[%image-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.		
[%image-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.		
[%block-category %]	This tag will be replaced with the name of the category of the page.		
[%powered-by%]	The tag will be replaced with the text: <table border="1" data-bbox="427 1350 1173 1400"> <tr> <td>Powered by</td> <td>NetOp Netfilter (c) 2007, Danware A/S</td> </tr> </table>	Powered by	NetOp Netfilter (c) 2007, Danware A/S
Powered by	NetOp Netfilter (c) 2007, Danware A/S		
{%blocked-url %}	This tag will be replaced with the URL that was blocked.		
{%timestamp %}	This tag will be replaced with the time the page was blocked.		

**Note:**

[%...%] These tags must be placed on a line of their own.  
 {%...%} These tags may be placed in the text as desired.

### 4.5.4 Cache

**Reset** NetOp Netfilter stores visited pages in a cache to improve speed when the pages are visited again. Use this function to delete the contents of the [cache](#).

## 4.5.5 Time schedule

NetOp Netfilter allows you to vary some of the settings according to a [time schedule](#). These settings include whether a particular segment has access to the Internet, whether filtering is activated, and, if it is, what to block.

When the time schedule is empty, the settings specified in the main window (as described in the previous sections) will be used. When settings have been specified for a block in the time schedule, these will override the settings specified in the main window.

<b>Adding a block to the schedule</b>	Settings for a block in the time schedule can be added by clicking on the time slot for the start of the period and then, while keeping the mouse button pressed down, dragging to mark the desired period. When the period has been marked, right-click on the marked area and select Add.... The contents of the window then changes to the settings panel.
<b>Choosing settings for block</b>	In the settings panel, you can adjust the start and end of the period and choose which days of the week the settings you are specifying should be applied. You can also choose which segments these settings should be used for, i.e. different segments may have different settings for the same period of time.
	The settings for the period you have selected are edited in the list at the bottom of the window. Refer to the previous sections for more information on these settings.
	When you have specified which settings that must be used, which segments they must be used for, and when they must be used, press APPLY. This will bring you back to the time schedule, where you can add new blocks, modify settings for existing blocks, and delete blocks.
<b>Editing and deleting blocks</b>	To modify the settings for a block, choose Edit... in the menu that appears when you right-click on the block. To delete a block from the time schedule, choose Delete in the menu.
<b>Displaying time schedule for a segment</b>	If you wish to see how the schedule is for a particular segment, select that segment in the drop-down box at the top of the window.

## 4.5.6 Accounts & Privileges

It is possible to create several user [accounts](#) and assign different [privileges](#) to different groups of users of Netfilter Admin.

In the upper part of the window, a list of group is shown. In the lower part, it is shown which group each user belongs to.

<b>Groups</b>	To create a new group, press 'Add'. This will bring up a new window where name, description, and privileges for the group are chosen. The same window can later be opened by selecting the group and choosing 'Properties'. Groups to which no users are assigned can be removed by pressing 'Remove'. A group can be assigned the privilege needed to modify the <a href="#">Always block list</a> and the <a href="#">Always grant list</a> or the privilege of unrestricted access to all settings.
<b>Users</b>	A new user may be added with the button 'Add' below the list of user accounts. In the window that is shown, name, password, group membership etc. is chosen. If the account automatically must expire after some time, check 'The account expires' and enter the date and time for expiry. As for groups, the

	properties for the user may be shown with 'Properties' and the user may be removed with 'Delete'.
--	---

See: [Accounts & Privileges](#).

# Index

## %

%block-category% 66  
 %blocked-url% 66  
 %filter-message% 66  
 %filter-report% 66  
 %image-back src="IMAGE URL"% 66  
 %image-view src="IMAGE URL"% 66  
 %powered-by% 66  
 %timestamp% 66

▪

.reg 24

## /

/autodetect 12  
 /blockhost=addr 12  
 /disableproxy 12  
 /local 12  
 /nolock 12  
 /proxyhost=addr 12  
 /proxyport=nnnn 12  
 /script=url 12  
 /sharedip 12  
 /unamehost=addr 12  
 /unlock 12

## [

[%block-category%] 45  
 [%filter-message%] 45  
 [%filter-report%] 45  
 [%image-back src="IMAGEURL"%] 45  
 [%image-view src="IMAGEURL"%] 45  
 [%powered-by%] 45

## {

{%blocked-url%} 45  
 {%timestamp%} 45

## A

Access Control List 62  
   Always filtered 42  
   Denied access 42  
   Unfiltered 42  
 Accounts & Privileges 67  
 ACL 42, 62  
 ACL Rule Hierachy 42  
 Active Directory 20  
 Add rule 42  
 Add Users to Group 20  
 Adding a single-IP rule 62  
 Adding an IP-range rule 62  
 Admin port 53  
 Always block list 31, 53, 57

Always grant list 30, 53, 57  
 Amount of data processed 51  
 Authenticated Users 20  
 Auto discover 40  
 Auto-Logout 43  
 Automatic browser configuration 20, 22  
 Avg. bytes/sec 50  
 Avg. hits/sec 50

## B

blacklist 54  
 Block all MP3 37  
 block list 31  
 Block page 66  
 Blocked hits 50  
 Bytes processed 56

## C

Cache 66  
 Categories 57  
   Copyright violations 32  
   Dating 32  
   Gambling 32  
   Hate, racism and discrimination 32  
   Illegal or dangerous activities 32  
   Pornography 32  
   Violence and vulgar humor 32  
 Change Password 43  
 Change the database 43  
 Change Username 43  
 Chat  
   Adding a program 58  
   Allow all 34  
   Allow all defaults 34  
   Block all 34  
   Block all defaults 34  
   Program list 58  
   Removing a program 58  
 Citrix 39  
 Client commands 44, 64  
 Client connections 50  
 Config backup 36  
 Configuration Tool 12  
   Chat blocking 14  
   Full installation 14  
   Minimal installation 14  
   Name logging 14  
   Peer-2-peer blocking 14  
 Configure 'Netfilter Off' Group Policy 22  
 Contact information 7  
 Create Group Policy 20  
 Create Groups 20  
 Customer service 7

## D

Database 28  
 Deleting an ACL rule 62  
 Deploy Clients 20

Disable filter completely 36, 53

## E

ECLIENT.EXE  
  proxy settings 12  
Exceptions 20  
External proxy server 52

## F

Filename/ext's  
  Adding rules 59  
  Block common streaming media types 59  
  Removing rules 59  
Filter Port 52  
Filter Topic 27  
FilteredUsers 20, 22  
Filtering server hostname and status 56  
Filters 56  
Finish 22  
Firewall 12  
Full Installation 17

## G

General 36  
  Config backup 59  
  Disable filter completely 59  
  Network setup 59  
Granted hits 50  
Granted list 53  
Group policies 20  
Group Policy 20

## H

Help pages 56  
History 28  
Hits being processed 51  
HTML Tag 45

## I

Identification of clients 62  
Inappropriate content 6  
Interactive client commands 64  
Internet access 52  
Internet Access Proxy IP and description 56  
Internet Explorer 39  
IP address 42  
IP range 42  
IPCALC 28

## L

Language 66  
Large files  
  Block files larger than 59  
  Enable large file detection 59  
Local log 28  
localhost 10, 26  
Log 56

Log setup 39  
  Clients share same IP 59  
  Log DNS names 59  
  Log IP addresses 59  
  Log user names 59  
Login 26  
  Administrator password 56  
  Administrator username 56  
  Remote Server Address 56

## M

Match by substring 58  
Max. bytes/sec 50  
Max. hits/sec 50  
Minimal Installation 15  
Monitor Load 51  
MP3 analysis 37  
  Block all MP3 data 59  
  Enable MP3 detection 59  
MP3 detection 37

## N

name Group Policy 20  
Navigation in NetOp Netfilter Admin 27  
Netfilter Admin settings 43, 65  
Netfilter Inet-access Proxy 52  
Netfilter Inet-access Proxy settings  
  Description 63  
  IP 63  
  Port 63  
Netfilter Off 20, 22  
Netfilter On 20  
Netfilter Proxy 52  
Netfilter servers 36  
netfilter.adm 20  
NETFILTER\_9X\_OFF.REG 24  
NETFILTER\_NT\_OFF.REG 24  
NetOp Netfilter Test 10  
Network Setup 36  
  Manage Servers 61  
  Transfer Settings 61  
Norton Internet Security 53

## O

Open sessions 50  
original settings 24

## P

P2P 57  
Peer-2-peer  
  Adding a program 57  
  Allow all/default 33  
  Block all/default 33  
  Large Files 33  
  Piracy 33  
  Program list 57  
  Removing a program 57  
  Substring matching 33

- Permit All 53
- Port 3128 10
- Position of ACL rules 62
- Privileges 67
- Proxy 53
  - Admin Port 63
  - Filter Port 63
  - On/Off toggle 63
  - Server address 63
- proxy server 9, 39
- Proxy settings 20, 22, 36

## R

- Remove a rule 42
- Remove rule 42
- Reset Password 23
- Reset Username 23
- Results 56

## S

- Scripts folder 24
- SEARCH LOG 28
- Searching in a database 28
- Searching in log files 28
- Segments
  - Adding segments 61
  - DNS suffixes 40
  - Groups 40
  - IP addresses 40
  - Modifying and deleting segments 61
  - Testing segment definitions 61
  - User names 40
- Sensitivity
  - High 35, 59
  - Low 35, 59
  - Normal 35, 59
- Service started 56
- Setup 36, 59
- Show advanced settings 53
- SHOW LOG 28
- SQL editor 28
- Statistics
  - The bytes/sec graph 64
  - The hits/sec graph 64
  - The numerical data 64
  - Update frequency 64
- Statistics page 28
- Statistics Topic 50
- Status 56
  - Filtering 28
  - Internet proxy 28
  - Machine and port 28
  - Statistics 28
  - Version number 28
- System Requirements
  - Clients 9
  - Proxy 9
  - Server 9
  - Software support 9

## T

- Template 66
- Terminal Services 39
- Testing the ACL rule list 62
- Time schedule 47, 67
- Total bytes 50
- Total hits 50
- Translate an address 28

## U

- UnfilteredUsers 20, 22
- UnfilteredUsers group 22
- Uninstall Minimal Installation 24
- URL Lists 30
- URLs
  - Adding an URL 57
  - Removing an URL 57
- User accounts 67
- user management 20

## V

- Version 56