Cyclope Internet Filtering Proxy

- User Guide -

1. Overview

Cyclope Internet Filtering Proxy monitors the entire Internet traffic and blocks the access to websites and files according to the chosen filter. The requested web pages are displayed only if they comply with the specified filters.

Cyclope Internet Filtering Proxy comes to help companies better manage Internet usage and bandwidth consumption, reduce web browsing for personal use during working hours, eliminate explicit content websites form being accessed, protect the network against online threats, and discourage the download of unlicensed software and other copyrighted materials.

Cyclope Internet Filtering Proxy monitors the entire Internet traffic and blocks the access to websites and files according to the chosen filter. The requested web pages are displayed only if they comply with the specified filters.

Cyclope Internet Filtering Proxy is also an Internet Sharing Software, capable of providing cost effective Internet access to multiple computers via a single Internet connection.

2. Cyclope Internet Filtering Proxy User Interface

2.1 Login

The application web interface is available accessing: web.filter on your browser. For the moment, the interface supports only Internet Explorer browser.

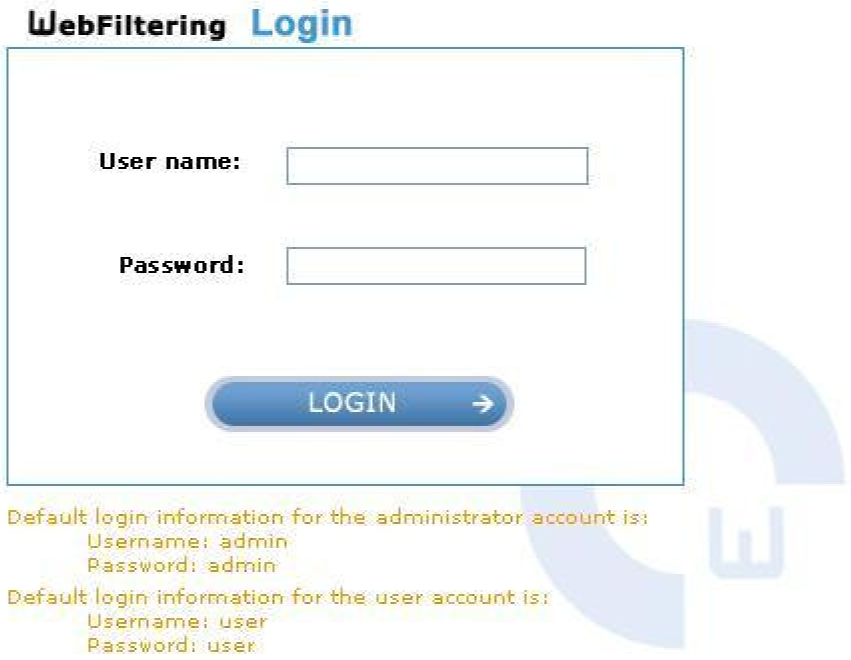
Default login details for the Administrator account are:

- Username: admin
- Password: admin

Default login details for the User account are:

- Username: user
- Password: user

All these details can be changed / modified once you are logged in form the Administration/Account panel.



Default login information for the administrator account is:
Username: admin
Password: admin
Default login information for the user account is:
Username: user
Password: user

2.2 Logout

For logging out, press the Logout button on the right upper corner of the interface.

3. Administration

3.1 IP Management

In the administration field, the application administrator sets the machines to be monitored. The monitored machines are available in an IP list containing IP addresses, and computer names.

Add an IP

In order to filter the Internet traffic on other machines you have to configure their proxy settings to use our product as proxy server. The settings for all browsers installed on client machines should be changed.

After you changed the proxy settings we recommend you to load a few web pages and see if they are loading correctly. If so, the client configuration is completed and you will be able to see the IP addresses of the client machines in the table above.

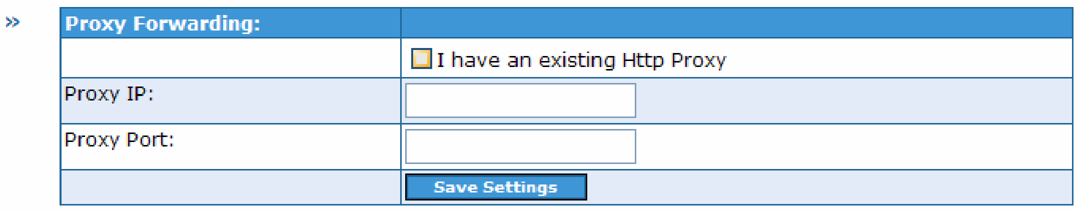
Delete IP

- Press the Delete IP Address to delete an IP.
- Press the Delete All button to delete all IP except the IP of the computer you are using.

Note: A deleted IP address will be automatically added in the list if the computer using that IP address is still configured to use our product as proxy server. So we recommend you to change the proxy server settings on the machines that are removed from the list.

3.2 Proxy Forwarding

If you already have an http proxy server that shares the Internet Connection in your LAN you can configure our product to forward the http requests to that proxy.



Proxy Forwarding:	
	□ I have an existing Http Proxy
Proxy IP:	
Proxy Port:	
	Save Settings

You have to enter the **IP address** and the **Port** of the existing http proxy and check the "I have an existing Http Proxy" option in order to configure our product to forward all the web requests received by our product to the already existing proxy. Our product will do the filtering part before sending the requests to the existing proxy server or after receiving the content from the existing proxy server (before sending the content to the final client). By using this feature our product filtering capabilities remain unchanged.

If you do not have an existing proxy server please do not use this feature by checking options or filling data.

3.3 Log Management

For better dating the user activity and log storage management, Cyclope Internet Filtering Proxy provides the possibility of choosing a specified day from a calendar. It has also two quick buttons: Delete Day Logs (erases a specified day logs) and Delete All Logs (erases all currently stored logs).

Logs are presented in a log list, containing IP address, computer name, date, log size, and delete log button. The delete button was inserted for a better space management.

Note: The daily logs are automatically removed after 3 months and after the containing data is aggregated in weekly, monthly and yearly reports.

3.4 Accounts

There are two types of accounts:

- Administrator account
- User account

When you are logged as an Administrator there are no restriction regarding the functionality of Cyclope Internet Filtering Proxy.

The User account allows only the viewing of the Cyclope Internet Filtering Proxy Statistics section.

This field contains the registration details and the login information.

Default login information for the Administrator account is:
Username: admin
Password: admin

Default login information for the User account is:
Username: user
Password: user

Login Change - fill in the fields

- Please choose the account type (Administration or User)
- New Password
- Retype Password

Note: Only the login password can be changed for users and administrators. The login names that are allowed by our product are admin and user – no new logins can be created.

4. Filter Configuration

Cyclope Internet Filtering Proxy allows multiple filters enabling for increased network protection. Filters can be a specific web page, a keyword, a group of letters, and an extension or file type.

The Filter Configuration section allows you to configure the filters, to monitor their status and to manage the different groups.

The divisions of this section are:

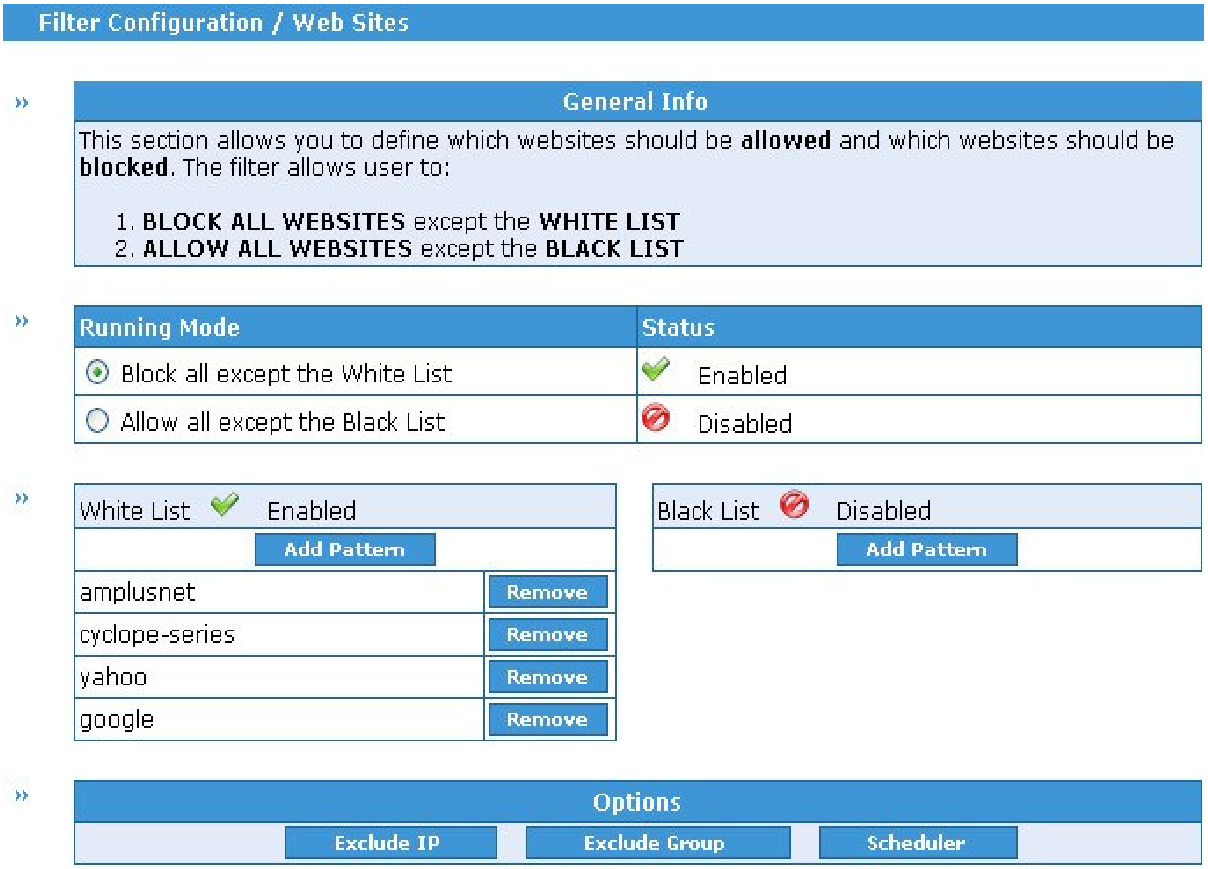
1. **Web Sites**- blocks URL from being displayed.
2. **Keywords & Profiles**- blocks a web page containing a specified word from being displayed.
3. **Files & Extensions**- blocks access to different file types (archives, applications, audio-video, etc.)
4. **Web Objects** - Block Shockwave and Flash objects from running, incoming cookies from being set on your computer and outgoing cookies from being read from your computer.
5. **Group Management** – allows the application administrator to create different groups of users.

4.1 Web Sites:

This filter blocks access to a specified web site or all web sites. In case of multiple websites on the same topic, the option Add pattern can be configured, enabling the filter to block all websites containing a keyword or a group of letters.

In the **Web Sites** filter section there are 2 running modes available:

- **Block all** except the **White List**– by checking this Running Mode, the user will be authorized to browse only the websites added in the white list. The rest of the websites will be blocked**.** The **Add Pattern** option assures you that all websites containing the specified pattern will be allowed (like groups.google.com not only google.com).



Filter Configuration / Web Sites

General Info

This section allows you to define which websites should be **allowed** and which websites should be **blocked**. The filter allows user to:

1. **BLOCK ALL WEBSITES** except the **WHITE LIST**
2. **ALLOW ALL WEBSITES** except the **BLACK LIST**

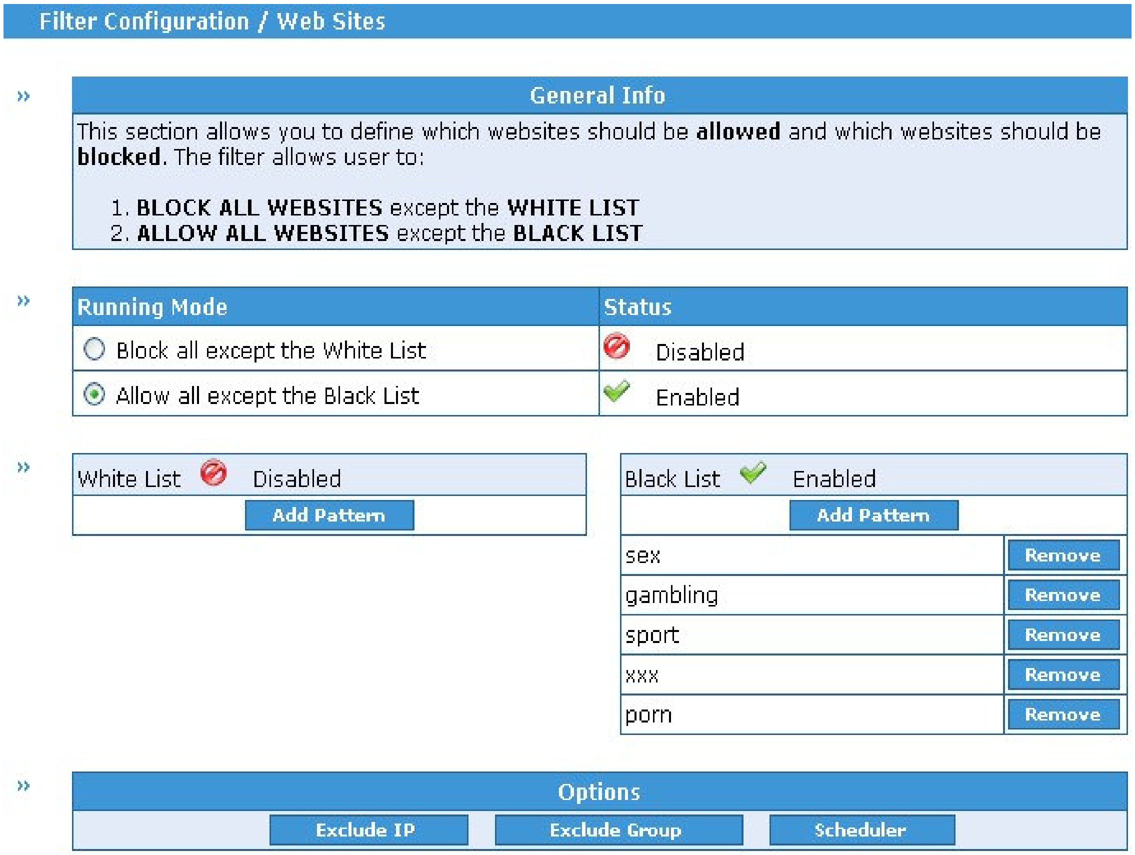
Running Mode	Status
● Block all except the White List	✓ Enabled
○ Allow all except the Black List	⊘ Disabled

White List ✓ Enabled

amplusnet	Remove
cyclope-series	Remove
yahoo	Remove
google	Remove

Black List ⊘ Disabled

- **Allow all** except the **Black List –** by checking this Running Mode, the websites added in the black list will be blocked. The **Add Pattern** option assures you of blocking access to a range of website containing specified pattern in the url: Example: if you add xxx as pattern – all website containing xxx in the url will be blocked.



Filter Configuration / Web Sites

General Info

This section allows you to define which websites should be **allowed** and which websites should be **blocked**. The filter allows user to:

1. **BLOCK ALL WEBSITES** except the **WHITE LIST**
2. **ALLOW ALL WEBSITES** except the **BLACK LIST**

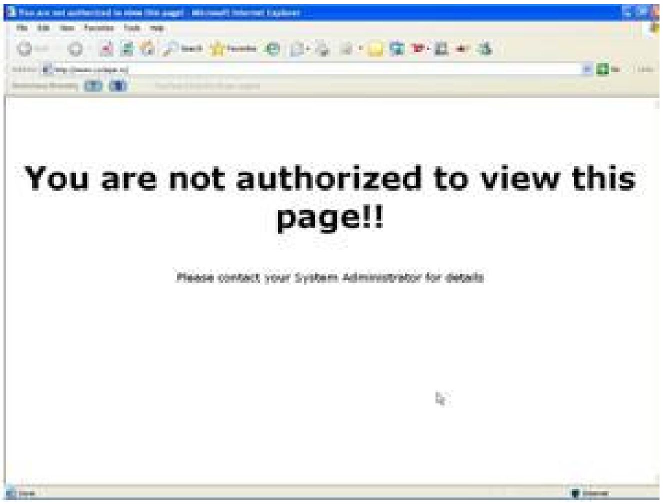
Running Mode	Status
○ Block all except the White List	⊘ Disabled
● Allow all except the Black List	✓ Enabled

White List ⊘ Disabled

Black List ✓ Enabled	
sex	Remove
gambling	Remove
sport	Remove
xxx	Remove
porn	Remove

For better property management, in case of changes in the word pattern contained in the sites to block you can access the **Remove** option.

The user will see the following message:



You are not authorized to view this page!!

Please contact your System Administrator for details

Note: For information about building custom error / blocked access pages contact our support team (support@cyclope-series.com).

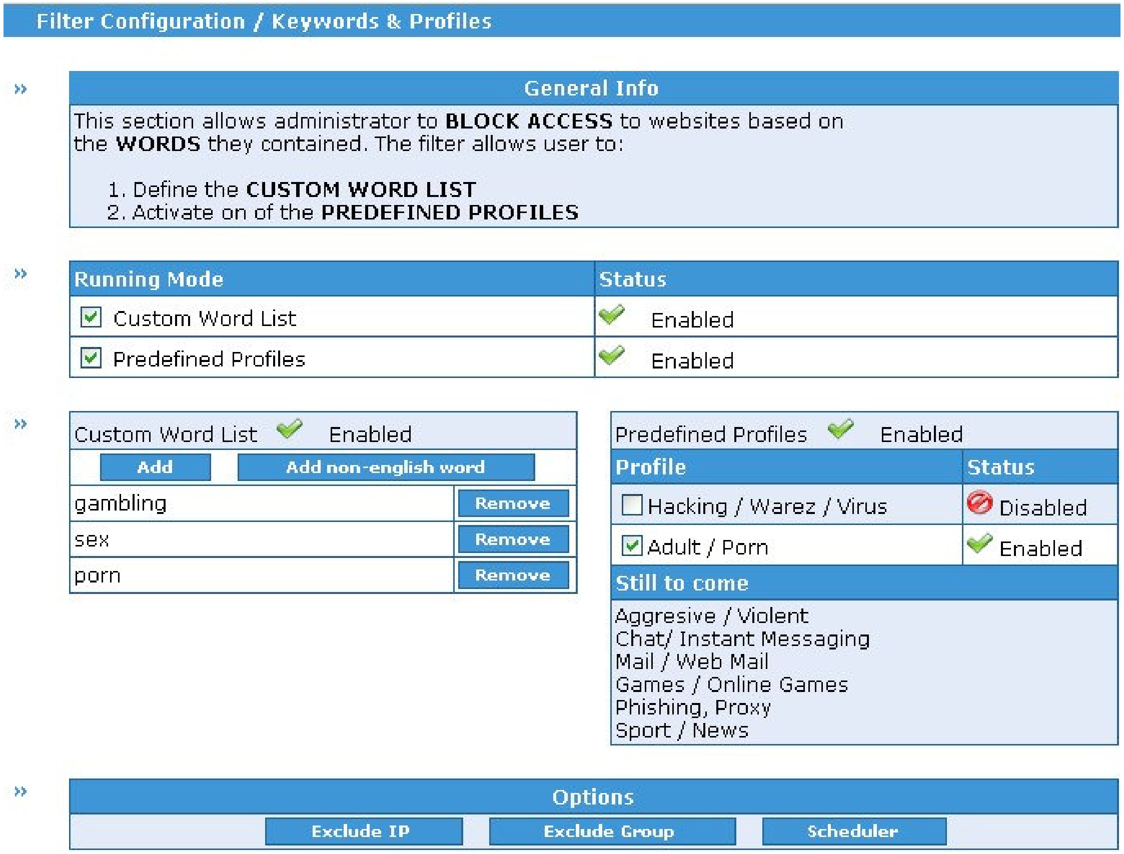
Options

- **Exclude IP –** the chosen IP is no longer monitored.
- **Exclude Group** – the chosen Group is no longer monitored.
- **Scheduler** – choose the time period for the filter action.

4.2 Keywords & Profiles

For enhanced protection, Cyclope Internet Filtering Proxy has a keyword filter, meaning that it stops web pages containing in their body a specified word or a group of letters from being displayed.

In the **Keywords & Profiles** filter section you can choose to create your own **Custom Word List** and/or to use the **predefined profiles** provided by Cyclope Internet Filtering Proxy.



Filter Configuration / Keywords & Profiles

General Info

This section allows administrator to **BLOCK ACCESS** to websites based on the **WORDS** they contained. The filter allows user to:

1. Define the **CUSTOM WORD LIST**
2. Activate on of the **PREDEFINED PROFILES**

Running Mode	Status
☑ Custom Word List	✓ Enabled
☑ Predefined Profiles	✓ Enabled

Custom Word List ✓ Enabled

gambling	Remove
sex	Remove
porn	Remove

Predefined Profiles ✓ Enabled

Profile	Status
□ Hacking / Warez / Virus	⊘ Disabled
☑ Adult / Porn	✓ Enabled

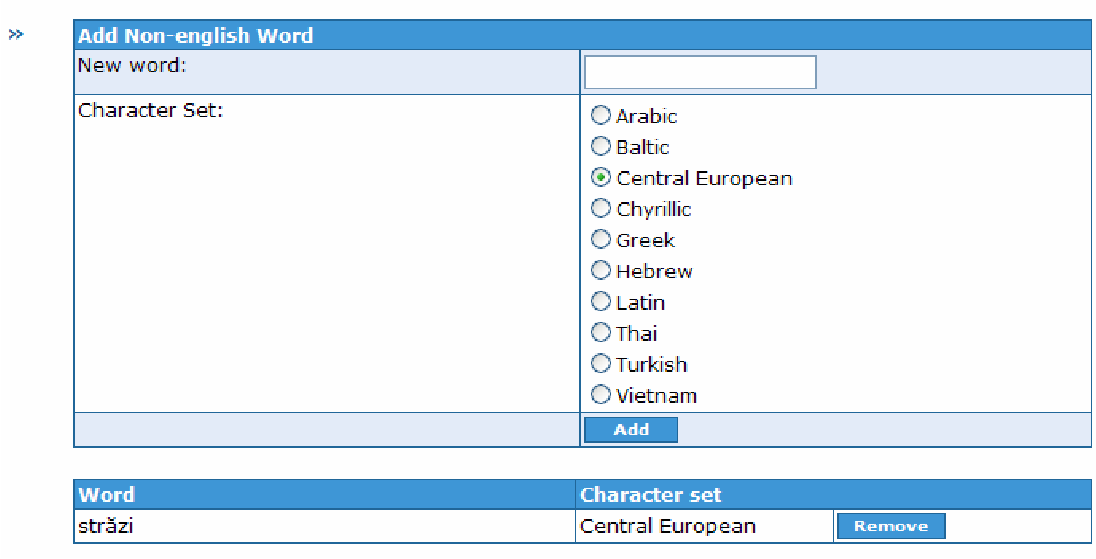
Still to come

Aggresive / Violent
Chat/ Instant Messaging
Mail / Web Mail
Games / Online Games
Phishing, Proxy
Sport / News

Options

- If you choose to define your own, **custom word list** use the **Add** button in order to create the block list. When the keyword is found in the website body, that website will be replace with a page containing restriction details.

The **Add non-english word** option, included in this filter, allows blocking the access to non-english web sites as well. The web sites containing the specified non-english word will not be displayed.



Add Non-english Word	
New word:	
Character Set:	○ Arabic ○ Baltic ● Central European ○ Chyrillic ○ Greek ○ Hebrew ○ Latin ○ Thai ○ Turkish ○ Vietnam
	Add

Word	Character set	
străzi	Central European	Remove

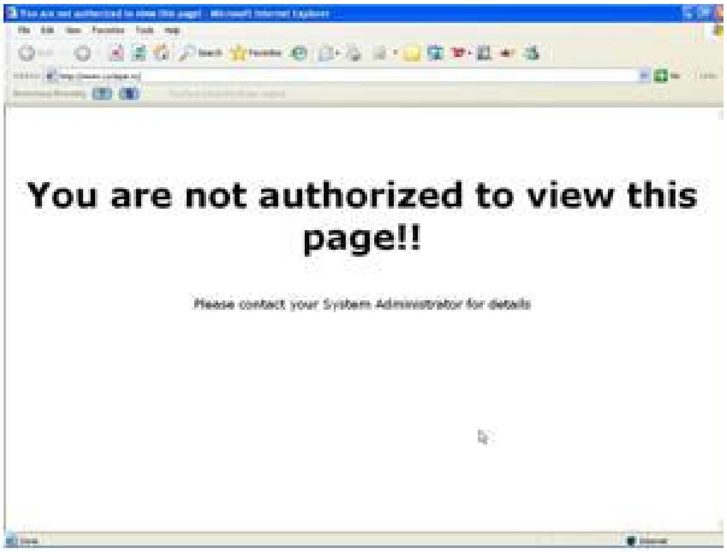
When selecting the character set please read the following:

- select **Chirillic** for Razeri, Belarusian, Bulgarian, FYRO Macedonian, Kazakh, Kyrgyz, Mongolian, Russian, Serbian, Tatar, Ukrainian, Uzbek, and Macedonian;
- select **Latin** for Afrikaans, Basque, Danish, Dutch, Faroese, Finnish, French, German, Icelandic, Irish, Italian, Malay, Norvegian, Portuguese, Scottish, Spanish, Swedish, Swahili;
- select **Central European** for Albanian, Croatian, Czech, Hungarian, Polish, Romanian, Serbian (Latin), Slovak, Slovenian;
- select **Baltic** for Lituanian, Latvian, Estonian;
- select **Arabic** for Arabic, Farsi, Urdu.

- If you choose the **predefined profiles** provided by **Cyclope Internet Filtering Proxy**, check the appropriate profile in order to enable it.

For better property management, in case of changes in the word pattern contained in the sites to block you can access the **Remove** option.

The user will see the following message:



You are not authorized to view this page!!

Please contact your System Administrator for details

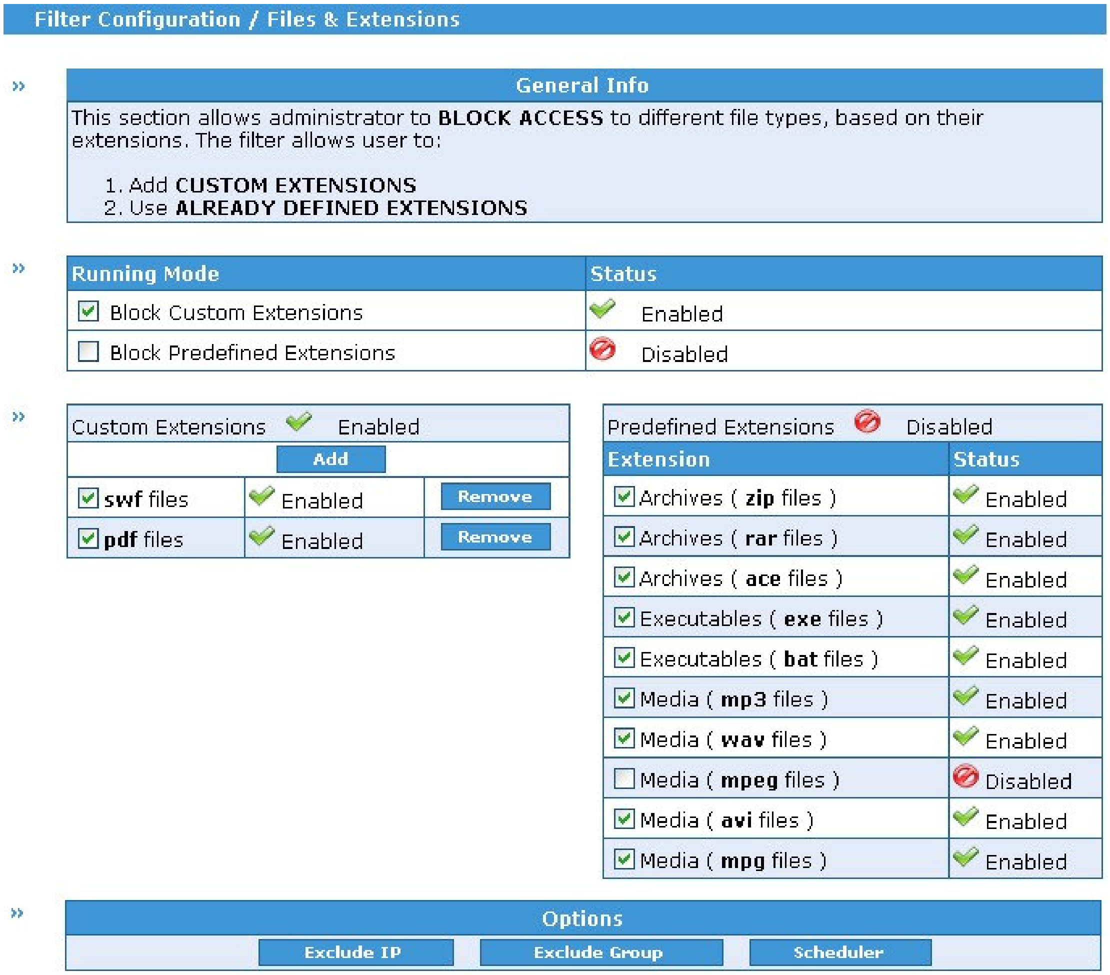
Options:

- **Exclude IP** – the chosen IP is no longer monitored.
- **Exclude Group** – the chosen Group is no longer monitored.
- **Scheduler** – choose the time period for the filter action.

4.3 Files & Extensions

In the **Files & Extensions** filter section you can choose to create your own **Custom Extensions List** and/or to use the already **defined extensions** provided by Cyclope Internet Filtering Proxy.

- If you choose to define your own, **custom extension list** use the **Add** button in order to create the block list.



Filter Configuration / Files & Extensions

»

General Info
This section allows administrator to **BLOCK ACCESS** to different file types, based on their extensions. The filter allows user to: 1. Add **CUSTOM EXTENSIONS** 2. Use **ALREADY DEFINED EXTENSIONS**

»

Running Mode	Status
☑ Block Custom Extensions	✓ Enabled
☐ Block Predefined Extensions	⊘ Disabled

»

Custom Extensions ✓ Enabled		
Add		
☑ **swf** files	✓ Enabled	Remove
☑ **pdf** files	✓ Enabled	Remove

Predefined Extensions ⊘ Disabled	
Extension	Status
☑ Archives (**zip** files)	✓ Enabled
☑ Archives (**rar** files)	✓ Enabled
☑ Archives (**ace** files)	✓ Enabled
☑ Executables (**exe** files)	✓ Enabled
☑ Executables (**bat** files)	✓ Enabled
☑ Media (**mp3** files)	✓ Enabled
☑ Media (**wav** files)	✓ Enabled
☐ Media (**mpeg** files)	⊘ Disabled
☑ Media (**avi** files)	✓ Enabled
☑ Media (**mpg** files)	✓ Enabled

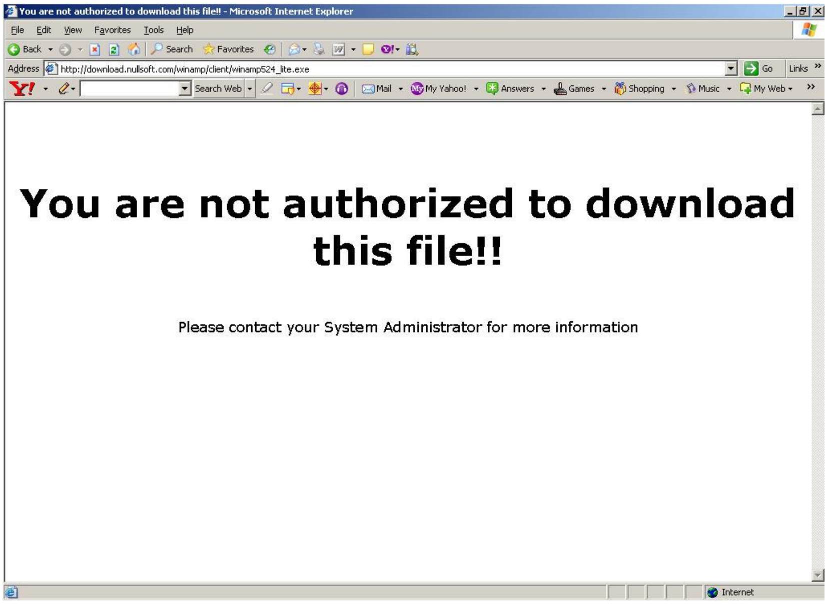
»

Options

Note: When a new extension is added – pdf for example you have to fill just the extension name (pdf). Using other combinations like .pdf or *.pdf is not supported and as result the access will not be blocked to the resources.

When blocking that type of file, the link will be redirected to an error page informing the blocked access to that specific file.

The user will see the following message:


You are not authorized to download this file!! - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://download.nullsoft.com/winamp/client/winamp524_lite.exe
Go Links
Search Web Mail My Yahoo! Answers Games Shopping Music My Web
Internet

You are not authorized to download this file!!

Please contact your System Administrator for more information

For better property management, in case you don't want to block an extension anymore, use the **Remove** option.

- If you choose the **predefined extensions** as a Running Mode, please check the appropriate extension in order to enable the filter.

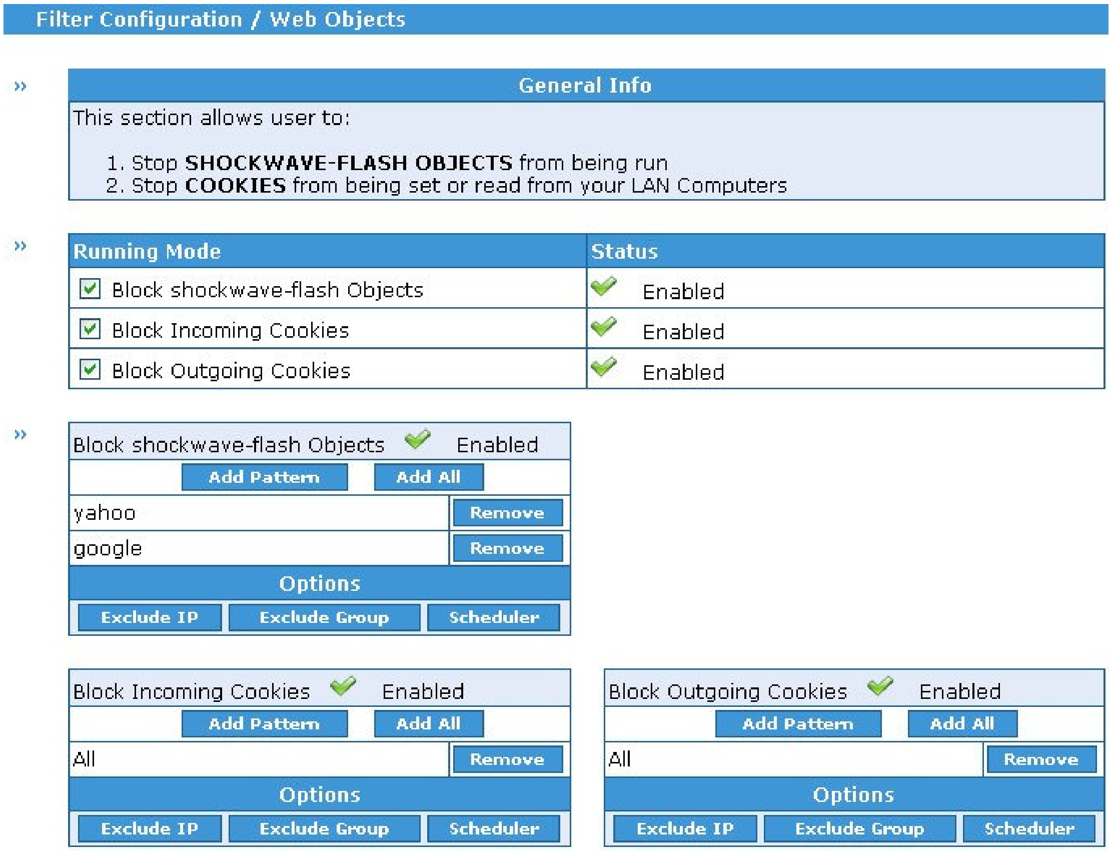
According to the chosen extension, the archive files, the applications and the audio-video files will be stop from being downloaded.

Options:

- **Exclude IP** – the chosen IP is no longer monitored.
- **Exclude Group** – the chosen Group is no longer monitored.
- **Scheduler** – choose the time period for the filter action.

4.4 Web Objects

This section allows administrator to stop **Shockwave-Flash Objects** from being run and to stop **Cookies** from being set or read from your LAN Computers.



Filter Configuration / Web Objects

General Info

This section allows user to:

1. Stop **SHOCKWAVE-FLASH OBJECTS** from being run
2. Stop **COOKIES** from being set or read from your LAN Computers

Running Mode	Status
☑ Block shockwave-flash Objects	✓ Enabled
☑ Block Incoming Cookies	✓ Enabled
☑ Block Outgoing Cookies	✓ Enabled

Block shockwave-flash Objects ✓ Enabled

yahoo	Remove
google	Remove

Block Incoming Cookies ✓ Enabled

All	Remove

Block Outgoing Cookies ✓ Enabled

All	Remove

In the **Web Objects** filter section there are three Running Modes available:

- **Block Shockwave-Flash Objects** - blocks the display of Shockwave and Flash applications within a web page. The content of the web site is loaded just the flash object is not shown.

- For defining the URL pattern, click **Add Pattern** button then write the letter group contained in websites you would like to block.
- **Add All:** by clicking this button, shockwave-flash objects from all websites will be blocked.

For better property management, the filter provides a **Remove** option.

- **Block Incoming Cookies** – This filter stops cookies from being set on a computer. It can be applied to a specified web page and also on web pages containing a keyword or a group of letters.

Cookies are usually set by web sites that need further user recognition or login details. It is recommended to check the login operation on these websites before blocking the access.

- For defining the URL pattern, click the **Add Pattern** button then write the letter group contained in websites you would like to block.
- **Add All:** by clicking this button, the incoming cookies for **all websites** will be blocked.

For better property management, the filter provides a **Remove** option.

- **Block Outgoing Cookies** – This filter stops cookies from being read from a computer. It can be applied to a specified web page and also on web pages containing a keyword or a group of letters.

Cookies are usually set by web sites that need further user recognition or login details. It is recommended to check the login operation on these websites before blocking the access.

- For defining the URL pattern, click the **Add Pattern** button then write the letter group contained in websites you would like to block.
- **Add All:** by clicking this button, the outgoing cookies for **all websites** will be blocked.

For better property management, the filter provides a **Remove** option.

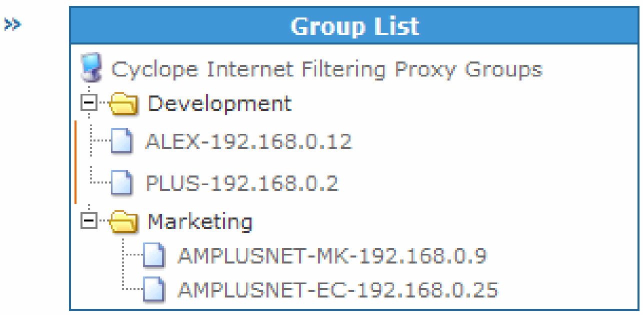
Options:

- **Exclude IP** – the chosen IP is no longer monitored.
- **Exclude Group** – the chosen Group is no longer monitored.
- **Scheduler** – choose the time period for the filter action.

4.5 Group Management:

Group Management allows application manager to create groups for different categories of users.

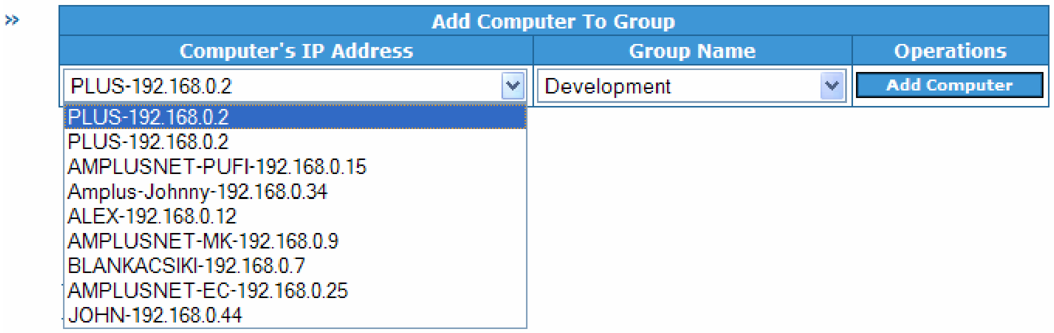
- **Add Group -** Create a new group for a specific category of users. After you include the computers' IP in each group, you will se a detailed list.



Group List

Cyclope Internet Filtering Proxy Groups
- Development
  - ALEX-192.168.0.12
  - PLUS-192.168.0.2
- Marketing
  - AMPLUSNET-MK-192.168.0.9
  - AMPLUSNET-EC-192.168.0.25

- **Add computer -** Assign computer/user to a specified group.



Add Computer To Group

Computer's IP Address	Group Name	Operations
PLUS-192.168.0.2	Development	Add Computer

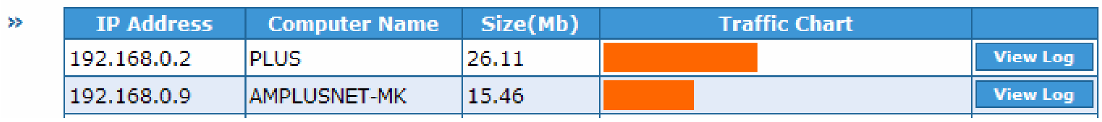
PLUS-192.168.0.2
PLUS-192.168.0.2
AMPLUSNET-PUFI-192.168.0.15
Amplus-Johnny-192.168.0.34
ALEX-192.168.0.12
AMPLUSNET-MK-192.168.0.9
BLANKACSIKI-192.168.0.7
AMPLUSNET-EC-192.168.0.25
JOHN-192.168.0.44

- **Delete Group -** Choose the group you want to delete.
- **Rename Group -** Choose the group you want to rename and enter the new name.
- **Delete Computer -** Delete user/computer from the specified group.

5. Statistics

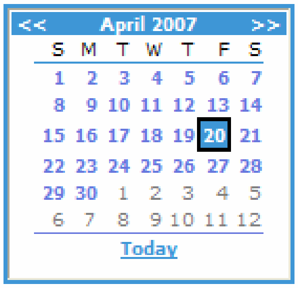
5.1 Traffic and Websites

After logging in, the page you are visualizing is the statistics page. Traffic & Website panel reports the IP activity and size (expressed in Megabytes - Mbytes) and chart in traffic. The **View Log** button allows you to see the accessed pages. Below the table, there is the total traffic made on the filtering proxy.



IP Address	Computer Name	Size(Mb)	Traffic Chart	
192.168.0.2	PLUS	26.11		View Log
192.168.0.9	AMPLUSNET-MK	15.46		View Log

Logs can be visualized on specified dates, choosing the date from the calendar above the table.



<< April 2007 >>

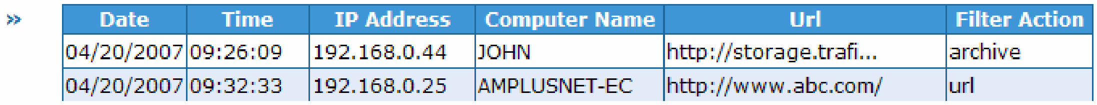
S	M	T	W	T	F	S
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5
6	7	8	9	10	11	12

Today

5.2 Filter Activity

The filter activity panel reports the results of the application usage. Filter activity reporting shows all filter activity and the breaking rules attempts.

The website visited and the action taken by Cyclope Internet Filtering Proxy are presented in a table format, accompanied by information on date, time, IP and computer name Filter action may be: URL blocked, download stopped, and incoming cookies blocked etc. Filter activity reports are available on daily basis.



Date	Time	IP Address	Computer Name	Url	Filter Action
04/20/2007	09:26:09	192.168.0.44	JOHN	http://storage.trafi...	archive
04/20/2007	09:32:33	192.168.0.25	AMPLUSNET-EC	http://www.abc.com/	url

5.3 Aggregated Traffic and Websites

Aggregated traffic logs provide detailed information on the traffic made by the monitored IPs for specific periods of time.

The period of time can be selected from the dropdown list, next to the chart. Time periods can be: this week, last two weeks, last months, last three months, last six months and last year. The table presents the monitored IPs, computers name, traffic size in Kb, and a graphical representation of the traffic made by that IP. Below the table is the total traffic made by the monitored IPs.

5.4 Aggregated Filter Activity

Aggregated Filter Activity logs provide detailed information on the filter activity made for specific periods of time. Filter table shows all active filters; in the case of file extension filters, only active extensions are shown. Aggregated filter activity report can cover specific periods of time, available to be chosen in the drop down list.

5.5 Reporting

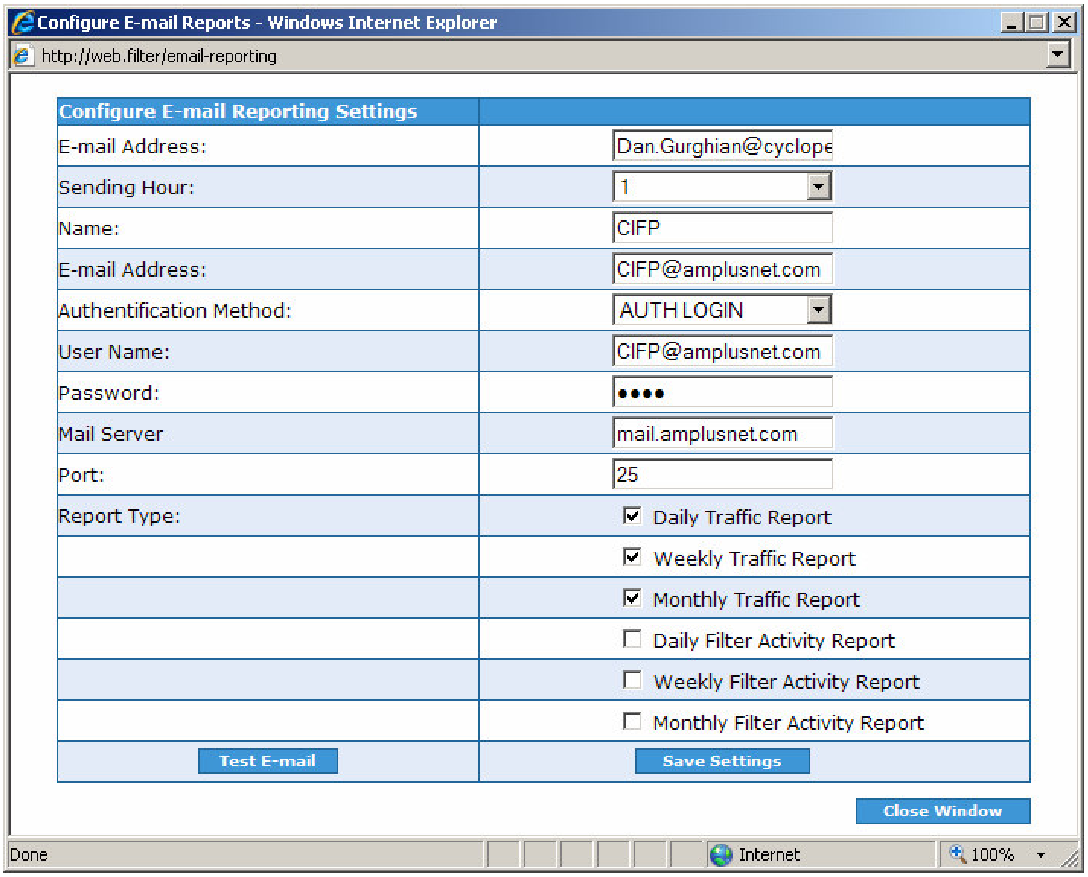
In the reporting section you have to configure the e-mail reporting settings so that you can receive the reports provided the Cyclope Internet Filtering Proxy solution.

By default the email reporting feature is configured to use our mail server to deliver you the reports. In order to test this feature please enter your email address in the first field and press Test E-mail button. Check your email and see if you have received an email from cifp@amplusnet.com with the subject Email Reports from Cyclope Internet Filtering Proxy and the attachment: test.zip.

Note:

Other options that can be configured are:

- the sending hour which allows you to specify when the emails should be sent,
- your own email server details:
    - Name – this is the information that will be present in the from field
    - E-mail Address – the email address that will be used for sending the email
    - Authentification Method that is supported by your SMPT server (the most common is AUTH LOGIN)
    - User Name – is the SMPT server username (usually is full email address)
    - Password – the password for the SMPT server
    - Mail Server – the name or the IP address of your SMP server
    - Port – the port used by your SMP server (the default value is 25)



Configure E-mail Reports - Windows Internet Explorer

http://web.filter/email-reporting

Configure E-mail Reporting Settings	
E-mail Address:	Dan.Gurghian@cyclope
Sending Hour:	1
Name:	CIFP
E-mail Address:	CIFP@amplusnet.com
Authentification Method:	AUTH LOGIN
User Name:	CIFP@amplusnet.com
Password:	••••
Mail Server	mail.amplusnet.com
Port:	25
Report Type:	☑ Daily Traffic Report
	☑ Weekly Traffic Report
	☑ Monthly Traffic Report
	☐ Daily Filter Activity Report
	☐ Weekly Filter Activity Report
	☐ Monthly Filter Activity Report
Test E-mail	Save Settings

- The types of the reports that you will receive by email:
    - Daily Traffic Report – this report will be delivered each day (at the hour that you have previously configured) and will contain the a table with all the IP addresses and the traffic (download and upload) for each of them;
    - Weekly Traffic Report – this report aggregates the daily logs and provides the same data (traffic size for each IP) for a week.
    - Monthly Traffic Report – this report aggregates the weekly logs and provides the same data (traffic size for each IP) for a month.
    - Daily Filter Activity Report – shows a table with the Date, Time, IP Address, Web Site and Filter Type that blocked the user access to a web resource.
    - Weekly Filter Activity Report – aggregates the daily reports into a single report
    - Monthly Filter Activity Report – aggregates the weekly reports into a single report

Use Save settings to validate your options.

6. Backup utility

Allows you to backup / restore your settings. This feature is useful for companies that have multiple instances of CIFP installed in order to have the settings (filtering policy) on all servers.

You can check which settings will be included in the backup:

- **Web Sites** (which websites are blocked and which are allowed; black list and white list)
- **Keywords & Profiles** (the list of blocked words and the profiles)
- **Files & Extensions** (the list of file types that are blocked)
- **Scheduler for the Filters** (if you have defined a scheduler for the filtering policy this can be included in the backup)
- **Rules for each IP** (the list of IP addressed that are excluded from the filtering policy)
- **Groups** (the group structure that you have defined)
- **Passwords** (user and admin passwords can be included in the backup).

When **Backup** Button is pressed a zip file is created and stored in to the application folder (usually c:\Program Files\CIFP). The zip file name is CIFPBackup_month_day_year.zip (example CIFPBackup_07_19_2007.zip).

When **Restore** button is pressed you will be able to select a zip file (named CIFPBackup_month_day_year.zip) from the installation folder (usually c:\Program Files\CIFP) which will be used to restore the settings. **Please note that the RESTORE will overwrite the existing settings with the settings (filtering policy, ip rules, passwords) stored in the backup file.**

7. Registration

In order to register your product, please go to: http://www.cyclope-series.com/products/internet-filtering/order.aspx. Before proceeding, make sure that you have disabled the product so that the payment processing service provider web page can be accessed without any restrictions. The license key and registration instructions will be sent by email.

8. Support

E-mail Support
For any technical related question please contact our technical support team: support@cyclope-series.com
For any sales related questions please contact our sales support team: sales@cyclope-series.com

Phone Support
Our phone support lines (available during working days):
+40 365 401269