

**This document provides information to install and use
WebScan for Linux**

User Guide WebScan for Linux

WebScan for Linux

END-USER LICENSE AGREEMENT FOR SOFTWARE.

IMPORTANT-READ CAREFULLY:

This WebScan End-User License Agreement ("EULA") is a legal agreement that you (either an individual or a single entity) have signed for the WebScan software product identified above, which includes computer software and associated media and printed materials, and may include "online" or electronic documentation ("SOFTWARE PRODUCT" or "SOFTWARE"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA.

SOFTWARE PRODUCT LICENSE

The SOFTWARE PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

The SOFTWARE PRODUCT is licensed, not sold.

1. GRANT OF LICENSE. This EULA grants you the following rights:

- a. You may use one copy of the WebScan Product identified above on a single computer for your personal use. The SOFTWARE is in "use" on a computer when it is loaded into temporary memory (i.e., RAM) or installed into permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that computer. However, installation on a network server for the sole purpose of internal distribution to one or more other computer(s) shall not constitute "use" for which a separate license is required, provided you have a separate license for each computer to which the SOFTWARE is distributed.
- b. Solely with respect to electronic documents included with the SOFTWARE, you may make an unlimited number of copies (either in hard copy or electronic form), provided that such copies shall be used only for internal purposes and are not republished or distributed to any third party.

2. OWNERSHIP.

Except as expressly licensed to you in this Agreement, MicroWorld retains all rights, title and interest in and to the SOFTWARE PRODUCT.

3. COPYRIGHT.

All title and copyrights in and to the SOFTWARE PRODUCT (including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the SOFTWARE PRODUCT), the accompanying printed materials, and any copies of the SOFTWARE PRODUCT are owned by its suppliers.

The SOFTWARE PRODUCT is protected by copyright laws and international treaty provisions.

Therefore, you must treat the SOFTWARE PRODUCT like any other copyrighted material except that you may either (a) make one copy of the SOFTWARE PRODUCT solely for backup or archival purposes or (b) install the SOFTWARE PRODUCT on a single computer provided you keep the original solely for backup or archival purposes.

You may not copy the printed materials accompanying the SOFTWARE PRODUCT.

Postfix Trademark & copyrights is owned by [Wietse Zweitze Venema](#)

AMaViSd-new Copyright is owned by [Mark Martinec](#) and others.

alterMIME Copyright is owned by Paul L Daniels - [AlterMIME](#).

Anteater Copyright is owned by [Tobias Erbsland](#).

AVPLite and AVP Trademark & copyrights is owned by Kaspersky Labs.

eScan and WebScan Trademark & copyrights is owned by [MicroWorld Software Services Pvt Ltd](#).

4. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS.

- a. Limitations on Reverse Engineering, Decompilation, and Disassembly. You may not reverse engineer, decompile, or disassemble the SOFTWARE, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation.
- b. Rental. You may NOT rent or lease the SOFTWARE PRODUCT.
- c. You must maintain all copyright notices on all copies of the SOFTWARE PRODUCT.
- d. You may not charge for distributing copies of the "Shareware versions" of the SOFTWARE PRODUCT to third parties. You may NOT distribute copies of the "registered versions" of the SOFTWARE PRODUCT to third parties.
- e. Software Transfer. You may permanently transfer all of your rights under this EULA, provided that you retain no copies, you transfer all of the SOFTWARE PRODUCT (including all component parts, the media and printed materials, any upgrades, this EULA, and, if applicable, the Certificate of Authenticity), and the recipient agrees to the terms of this EULA.
- f. Termination. Without prejudice to any other rights, MicroWorld may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE PRODUCT.

5. LIMITED WARRANTY

MicroWorld DOES NOT WARRENT THE ACCURACY OF ANY STATISTICS GATHERED BY THIS SOFTWARE.

The software and related manual are provided "as is." The supplier makes no representations or warranties with respect to the software and manual and disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The supplier reserves the right to make changes to any and all parts of the software at any time without notice.

MAILSCAN'S SUPPLIERS DISCLAIM ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH REGARD TO THE SOFTWARE PRODUCT.

IN NO EVENT SHALL MAILSCAN'S SUPPLIERS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE PRODUCT, EVEN IF MAILSCAN'S SUPPLIERS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This product contains Free and Open Source Softwares which are copyrighted by their respective authors. The licenses for the same are included with this product with appropriate ownership of the products.

Table of Contents

Welcome	6
FEATURES OF WEBSKAN FOR LINUX	6
CONTACT US	8
Installation	9
GETTING WEBSKAN FOR LINUX RPMs	9
INSTALLATION AND GETTING STARTED	10
SYSTEM REQUIREMENTS	10
INSTALLATION	11
CONFIGURATION	11
UNINSTALLATION	12
Server Control	13
SERVER CONTROL STATUS	13
SERVER CONTROL MANAGE ADMIN	15
General Settings	16
SERVER CONTROL - GENERAL SETTINGS	16
POPUP BLOCKER	19
AD FILTER	20
Content Filter	22
CONTENT FILTER - CATEGORIES	22
CONTENT FILTER WHITE LIST.....	24
CONTENT FILTER MIME TYPES	25
Pics Rating	26
PICS RATING RSACI	26
PICS RATING SAFE SURF	27
 WebScan For Linux User Guide	 4

PICS RATING ICRA	29
Virus Scanner	31
VIRUS SCANNER SETTINGS	31
VIRUS DEFINITION UPDATES	32
Server Logs	34
SERVER LOGS VIOLATION LOGS	34
SERVER LOGS WEBSCAN LOGS.....	35
SERVER LOGS WEBSCAN OPERATIONS LOGS	36
Help	37
ABOUT	37
CONTACTS	37
HELP INDEX	37

Welcome

WebScan for Linux brings the awesome Anti Virus and Content Security features of MicroWorld products to protect the internal clients/networks served by Linux based Proxy Servers and stop the threat at the gateway level.

There is no direct threat to GNU/Linux servers as such. But since GNU/Linux is becoming popular on Servers, Proxies and Gateways, there is a need for solution that works on the GNU/Linux Platform.

Also Server based products give centralized control of Policy deployment for clients require least or no modification of client computers. WebScan for Linux provides this solution. The application is an extremely powerful web-based application that is easily configurable.

Features of WebScan for Linux

Key Features of WebScan for Linux are given below:

- Works transparently with world's most popular Squid Caching Proxy
- Scan Web pages for Contents Policy Violations.
- Scan Web page for Virus, Worms, Trojan and other Malware.
- Scanning of HTTP and FTP Protocols and Instant Messengers traffic.
- Pop-up Blocker to remove annoying Pop-up Ads and save bandwidth.

- Ad filter to block ad servers.
- Pre-defined and Admin created content filtering Policies
- Black listing and White listing of IP Addresses
- Black listing and White listing of Domains
- Black listing and White listing of URLs
- Black listing of MIME (File) Types (Audio, Video, Pictures etc.)
- Blocking HTTP file uploads for Information Security
- PICS Site Ratings using RASCI, Safe Surf and ICRA
- State-of-the-Art Anti-Virus Scanner
- Auto and/or manual updates of Virus Databases
- Extensive reporting system for Policy Violations
- Web Based GUI Front-end for easy configuration and administration

Contact Us

We offer 24x7 support to our customers through e-mail, telephone and Chat.

Chat Support

- Chat with our support team at ‘**escanchat**’ using: AOL; MSN or Yahoo messenger service.

E-Mail Support

- If you have any queries about our products or have suggestions and comments about this guide, please send them to support@mwti.net.

<p>Head Office:</p> <p>MicroWorld Technologies Inc. 33045 Hamilton Court East, Suite 105 Farmington Hills, MI 48334-3385 USA Tel: (248) 848 9081/9084 Fax: (248) 848 9085</p>	<p>Asia Pacific:</p> <p>MicroWorld Software Services Pvt Ltd.. Plot No 80, Road 15, MIDC, Marol, Andheri (E), Mumbai, INDIA. Tel (91) - 22- 28265701 - 05 Fax (91) - 22-28304750</p>
--	---

For sales enquiry, e-mail: sales@mwti.net

For support enquiry, e-mail: support@mwti.net

Installation

This document provides information about the system requirements and installation process for WebScan for Linux.

Getting WebScan for Linux RPMs

WebScan for Linux consist of 3 RPMs.:

Web based Admin Module RPM

- MWAdmin-1.0-X.i386.rpm
- (Web based Admin Module is common for all MicroWorld GNU/Linux Products)

Anti-Virus Module RPM

- mwav-1.0-X.i386.rpm
- (Anti-virus Engine with Virus Databases is common for many MicroWorld GNU/Linux Products)

WebScan for Linux RPM

- WebScan-1.0-X.i386.rpm

You can download these RPMs from

- <ftp://ftp.microworldsystems.com/linux/webscan/>
- <ftp://ftp.microworldsystems.com/linux/>

Installation and getting started

WebScan for Linux is a complete Anti-Virus and Web Content filtering solution for GNU/Linux proxy servers like Squid. WebScan bundles easy to use Anti-Virus and Content filtering proxy. This high speed, high performance, stable and secure content filtering solution provides out-of-the-box deployment for GNU/Linux Proxy servers on the Internet gateways.

System Requirements

- Requires a Red Hat Linux 9 or better installed on the system.
- Requires 20 MB of free space on the systems for installation and 100 MB or more for the working.
- Requires Pentium III with 128 MB RAM or better depending on the number of users and traffic.
- Requires Squid Caching Proxy. This is generally available on your distributions installation media. To download the RPM of Squid go to

<http://www.squid-cache.org/mirrors>

- Requires sarg package. To download the RPM of sarg from <http://dag.wieers.com/packages/sarg/>

Installation

To install the WebScan for Linux, use following commands as “root” user

```
# rpm -ivh /path/to/rpm/MWAdmin-1.0-X.i386.rpm
# rpm -ivh /path/to/rpm/mwav-1.0-X.i386.rpm
# rpm -ivh /path/to/rpm/WebScan-1.0-X.i386.rpm
```

- If you have any other MicroWorld GNU/Linux products installed on the server, you will not require to install MWAdmin and mwav packages.
- This will install the required packages in their own folder (directory) “/opt/MicroWorld”. The install process will also configure and start Web based Configuration and Management application.

Configuration

- To Configure WebScan for Linux start a browser and go to:
https://<proxy_server_ip>:10443/
e.g. if your server's IP is 192.168.0.1, URL will be

<https://192.168.0.1:10443>

- This will prompt for an user name and password. Default user name and password is admin/admin.
- Before you can proceed to configure the WebScan, you need to get a valid license key from MicroWorld web site. Follow the instructions provided on each screen.
- To register on-line go to <http://www.mwti.net/linux/registrationlinux.asp>

Uninstallation

To remove WebScan for Linux from the system you can use following commands

```
# rpm -e WebScan
```

```
# rpm -e mwav
```

```
# rpm -e MWAdmin
```

- However, if any other MicroWorld GNU/Linux products are installed, MWAdmin and mwav are required packages for them and you should not uninstall MWAdmin and mwav packages.
- This will remove WebScan for Linux from the system. However all changed configuration files, quarantined files and logs will remain on the file systems.

Server Control

This section provides information to configure the WebScan server status and to specify new password.

Server Control Status

This screen provides a list of services that are running and that are shut down. You can restart the services you want. WebScan for Linux has two components: WebScan Server and the Anti-Virus Server. All of them should be always running.

In the screen, when a service is running, it is identified by a black tick mark. When a service is not running, it is identified by a red cross mark. To restart a service, click on the single green arrow. To stop a service, click the red square.

Screen elements are explained as below:

Service Name

The column lists services that are configured to run. E.g.: WebScan Server;
Anti-Virus Server

Service Status

This column displays the status. If the service is running then a box with a black check mark is shown. If a service has been stopped then a box with a Red X mark is displayed

Restart

A green arrow mark is displayed in the column against each service. If you wish to restart the service, then click the green arrow mark

Stop

A red square is displayed in the column against each service. If you wish to stop the service, then click the red square

View Log

To view the log of a service, click the document symbol. The Log menu screen is displayed

WebScan Server

This is the WebScan Server that scans accessed web pages and blocks harmful content.

Anti-Virus Server

This is the anti-virus server. The accessed web pages are scanned for viruses and when harmful content is detected, the page is blocked.

Server Control Manage Admin

This page allows you to change the administrators password of WebScan for Linux. After registering the product, it is recommended that you change the admin password. You need to enter the old password before entering the new one.

Screen elements are explained as below:

Change Admin Password:

Enter the **Old Password**, the **New Password** and re-enter the new password for confirmation.

Click **Change Password**.

General Settings

This section allows you to configure IPs. Attachments to block, create a white list of URLs, configure log settings. You can also create a white list of URLs and Domains where PopUps and Ads are allowed.

Server Control - General Settings

This page allows you to specify connectivity features of your proxy server like IP, port, binding port and the maximum number of simultaneous connections that are allowed.

You can also block IP addresses from being accessed when they are typed in the URL, block unresolved IP and ports and block file uploads or attachments. You can create a white list of URLs that are allowed to be accessed.

When users attempt to access sites or carry out actions you have blocked, a log of such violations can be made.

Screen elements are explained as below:

Settings

Proxy IP Address

Enter the IP address of your proxy server. This is the proxy server through which users access the Internet and send mails.

Proxy Port

Enter the port number of the proxy server. The proxy will listen for Internet traffic on this port.

Port to Bind

Enter the port number to which you bind the WebScan server. The port should be other than the privileged port and there should not be any service running on it

Maximum Simultaneous Connections Allowed

Enter the maximum number of connections that should be enabled Simultaneous. This limits the number of connections that are live at any point of time.

Block

Block IP addresses in URL

Some sites provide access only through the IP. Since they do not have a name, ordinary content security applications are not able to block the site when a IP number is entered. WebScan for Linux blocks access to such IPs.

Block unresolved IP addresses

Certain banned sites may have IPS that are unresolved. WebScan for Linux allows you to block such IPs.

Block Ports (space separated list)

Enter the port numbers that should be blocked. All accessed sites that connect to this port are blocked.

Block File Uploads or File Attachments through Web

Select the check box to block files from being mailed as attachments. This powerful feature of WebScan prevents data theft.

White List Upload URLs

Enter the url of sites through which attachments can be uploaded.

Log Settings

Logging Enable

Logs of violations are generated if the check box is selected.

Log Black Listed Url

When blocked urls are accessed or a url is blocked because of offensive content, a log file is generated if the check box is selected.

Log Blocked Port Access

You can block users from your network from accessing specific ports of remote servers. When your users try to access such blocked ports, a log file of such violations is generated.

Log IP addresses in URL

Some porn and other banned sites can be accessed only through their IP. A log of such IPs when they are entered in the url is created if the check box is selected.

Log Rating Violations

WebScan for Linux has incorporated website rating systems of different bodies like Safesurf, RASCI. When access sites violate these ratings a log is generated if the check box is selected.

Log Blocked Mime

Access to specific MIME types can be blocked. When such MIME types are accessed, a log is generated is the check box is selected.

Log Virus Infected Contents

When virus infected attachments are sent or downloaded, a log of such traffic is generated if the check box is selected.

Log Level

Log level defines the violation details that are displayed in the log. The drop-down lists number from 0 to 7, Zero means the bare minimum details are logged. Level 7 means that full details of the violations are logged

Activate Changes

After entering appropriate values in the above fields, click the button to activate them. A message is displayed in the top row giving status of your changes and warns you if invalid entries are made.

Reset

Clears recent changes made before you have activated the changes

Popup Blocker

A popup is an Ad or unsolicited information that appears on the accessed page and then in a separate popup window when you request for more information or inadvertently click on them. Popup's are exasperating and may not be relevant to your work. Besides consuming bandwidth, you waste browsing time in chasing and closing them. They offer a cheap way for companies to advertise their products.

WebScan Popup blocks all PopUp automatically. It tells your browser to stop all unsolicited windows from opening and does not interfere with your navigation. Since it stops the browser from downloading and showing PopUps, unlike most pop-up killers, there's no need to wait while a new window appears and disappears. It offers a screen flash free blocking of PopUp and saves your bandwidth.

Not all PopUps are unsolicited. You may need to fill in an on-line registration form, which is a type of popup. In such cases, you specify the website from which PopUps should be allowed. Such sites are included in the White List.

Screen elements are explained as below:

Enable

Select the checkbox to enable the feature of PopUp blocker.

White List

Domains

Enter the domain names whose PopUps should be allowed.

URLs

Enter the URLs whose PopUps should be allowed.

Activate Changes

After entering appropriate values in the above fields, click the button to activate them. A message is displayed in the top row giving status of your changes and warns you if invalid entries are made.

Reset

Clears recent changes made before you have activated the changes

Ad Filter

Online Advertisements are unsolicited information that appear on the accessed page and then in a separate popup window when you request for more information or inadvertently click on them. These are exasperating and may not be relevant to your work. Besides consuming bandwidth, you waste browsing time in chasing and closing them. They offer a cheap way for companies to advertise their products.

WebScan Ad Filter blocks such Ads from domains and URLs you specify. It tells your browser to stop all unsolicited windows from opening and does not interfere with your navigation. Since it stops the browser from downloading and showing Ads, unlike most ad killers, there's no need to wait while a new window appears and disappears. It offers a screen flash free blocking and saves your bandwidth.

Screen elements are explained as below:

Enable

Select the checkbox to enable the feature of Ad Filter.

List Of Adservers

Domains

Enter the domain names whose advertisements should be allowed.

URLs

Enter the URLs whose advertisements should be allowed.

Activate Changes

After entering appropriate values in the above fields, click the button to activate them. A message is displayed in the top row giving status of your changes and warns you if invalid entries are made.

Reset

Clears recent changes made before you have activated the changes

Content Filter

This section allows you to set content filters. You can create categories of restricted categories, create a white list of URLs and Domains and select the MIME types.

Content Filter - Categories

This page allows you to configure the content filters in your system. You can enable content filter to control access to sites accessed by your users. You can also enable the black list of banned URLs and when an offensive URL is detected, it can be added to the black list.

Even benign or useful sites can have words like sex, gambling, etc, Since they should not be blocked you can specify the number of times such words can occur before they are blocked.

Screen elements are explained as below:

Content Filter Enable

Select the check box to activate the content filter.

Black List URL Enable

Select the check box to activate the black list of banned URLs. When such URLs are accessed, they are automatically blocked.

Add Offensive URL to Black List

When a URL with offensive words is detected, it can be automatically blocked if the check box is selected. The URL is also added to the block list.

Unique Phrases Occurrences for blocking a page

Unique phrases associated with porn, gambling and other banned sites can also occur in legitimate sites. However, in legitimate sites they usually occur just a few times while in banned sites they occur many times. You can set a limit for the number of times such words and phrases occur. When the limit is crossed, then the accessed site is regarded as a banned site and blocked by WebScan

Categories

Important Content Filter categories are created for you. Banned words, blocked URLs are assigned to their respective categories. For e.g. Sex, Horny would appear in the Pornography category while Poker, blackjack would appear in the Gambling category. You can create additional categories as required. The four default categories are:

Pornography

Chat

Gambling

Classified

Click on the categories to see the list of Phrases, Domains and URLs associated with them and to edit if required. Deselecting the checkbox can deactivate a category.

Add New Category

You can add a new category to the content Filter. To add a new category, enter the name in the field and click activate changes. A message giving the status of this change, Success or Fail is displayed in the top frame. If successful, the new category is displayed in the list.

Activate Changes

After entering appropriate values in the above fields, click the button to activate them. A message is displayed in the top row giving status of your changes and warns you if invalid entries are made.

Reset

Clears recent changes made before you have activated the changes

Content Filter White List

White list contains a list of URLs and Domains for whom access is allowed. This page allows you to create a list of such sites and include them in the white list.

Enable White Listing

Select the check box to enable white list of allowed URLs. When the check box is selected, the white list of URLs is activated

White List

There are two list boxes that allow you to specify the URLs and the Domains that need to be included in the white list

URLs: Enter the URLs for whom access is allowed

Domains: Enter the Domains for whom access is allowed

Activate Changes

After entering appropriate values in the above fields, click the button to activate them. A message is displayed in the top row giving status of your changes and warns you if invalid entries are made.

Reset

Clears recent changes made before you have activated the changes

Content Filter MIME Types

This page allows you to specify the file MIME types that should be blocked. Enter the MIME type in the dialog box and click activate changes.

Enable MIME Types

Select the check box to enable the check for MIME types

MIME Types

Default MIME types are listed in the list box. You can modify or add to the list

Activate Changes

After entering appropriate values in the above fields, click the button to activate them. A message is displayed in the top row giving status of your changes and warns you if invalid entries are made.

Reset

Clears recent changes made before you have activated the changes

Pics Rating

This section allows you to prescribe safe browsing standards as specified by International rating agencies.

Pics Rating RSACi

WebScan allows you to choose The Recreational Software Advisory Council rating service for the Internet that prescribes filtering norms for safe browsing. You can specify threshold settings for various categories of content. RSACi is based on the work of Dr. Donal F. Roberts of Stanford University, who has studied the effects of media for nearly 20 years. Select the appropriate values from the drop-down list to assign the filter options.

Screen elements are explained as **below**:

Enable

Select the checkbox to enable the feature of RSACi Filter.

Language

Select the threshold values for language, listed in the drop-down list. The values range from Inoffensive to Crude Vulgar Language.

Nudity

Select the threshold values for Nudity, listed in the drop-down list. The values range from No Nudity to Provocative Display.

Sex

Select the threshold values for Sex, listed in the drop-down list. The values range from None, Innocent Kissing to Explicit Sexual Acts.

Activate Changes

After entering appropriate values in the above fields, click the button to activate them. A message is displayed in the top row giving status of your changes and warns you if invalid entries are made.

Reset

Clears recent changes made before you have activated the changes

Pics Rating Safe Surf

WebScan allows you to choose the SafeSurf Surf Rating Standard, designed with input from thousands of parents and Net citizens to empower each family to make informed decisions concerning accessibility of online content. You can specify threshold settings for various categories of content.

Screen elements are explained as below:

Enable

Select the checkbox to enable the feature of Safe Surf Filter.

Age Range

Select the age range for whom the Safe Surf standards should be set, from the values listed in the drop-down list. The values range from All Ages to Explicitly for Adults.

Heterosexual Themes

Select the threshold values for Heterosexual Themes, from the values listed in the drop-down list. The values range from Subtle Inuendo to Explicit.

Homosexual Themes

Select the threshold values for Homosexual Themes, from the values listed in the drop-down list. The values range from Subtle Inuendo to Explicit.

Profanity

Select the threshold values for Profanity, from the values listed in the drop-down list. The values range from Subtle Inuendo to Explicit.

Nudity

Select the threshold values for Nudity, from the values listed in the drop-down list. The values range from Subtle Inuendo to Explicit.

Violence

Select the threshold values for Violence, from the values listed in the drop-down list. The values range from Subtle Inuendo to Encouraging Personal Participation.

Sex

Select the threshold values for Sex, from the values listed in the drop-down list. The values range from Subtle Inuendo to Explicit.

Intolerance

Select the threshold values for Intolerance, from the values listed in the drop-down list. The values range from Subtle Inuendo to Advocating Violent or Hateful Actions.

Other Adult Themes

Select the threshold values for Other Adult Themes, from the values listed in the drop-down list. The values range from Subtle Inuendo to Explicit.

Glorifying Drug Use

Select the threshold values for Glorifying Drug Use, from the values listed in the drop-down list. The values range from Subtle Inuendo to Soliciting Personal Participation.

Activate Changes

After entering appropriate values in the above fields, click the button to activate them. A message is displayed in the top row giving status of your changes and warns you if invalid entries are made.

Reset

Clears recent changes made before you have activated the changes

Pics Rating ICRA

WebScan allows you to choose the ICRA Rating System Internet Content Rating Association. This is a global, cross-cultural rating and filtering system.

You can specify threshold settings for various categories of content.

Screen elements are explained as below:

Enable

Select the checkbox to enable the feature of Safe Surf Filter.

Chat

You can select the type of chatting that is allowed

Language

You can select the degree of profanity that the accessed site can have after which it is blocked.

Nudity & Sexual Material

You can select the degree of nudity and sexual content that the accessed site can have after which it is blocked.

Other Topics

Select from the list of topics that should be monitored.

Violence

Select from the list of topics related to violence that the accessed site can have after which it is blocked.

Activate Changes

After entering appropriate values in the above fields, click the button to activate them. A message is displayed in the top row giving status of your changes and warns you if invalid entries are made.

Reset

Clears recent changes made before you have activated the changes

Virus Scanner

This section allows you to specify MIME types that should not be scanned and also configure settings for automatic download of updates.

Virus Scanner Settings

This screen allows you to specify the MIME types that should not be scanned for viruses. Certain MIME types like images, pdf. etc. cannot carry viruses. To save time, such MIME types can be exempt from virus scan.

Screen elements are explained as below:

Enable

Select the checkbox to enable the feature of Virus Scanner

MIME Types that should not be scanned for virus

Enter the MIME Types in the dialog box that should not be scanned for viruses.

Activate Changes

After entering appropriate values in the above fields, click the button to activate them. A message is displayed in the top row giving status of your changes and warns you if invalid entries are made.

Reset

Clears recent changes made before you have activated the changes

Virus Definition Updates

Updates are vaccines that detect and remove new viruses. Each month about 50 new viruses are found. Your system must have the means to identify new viruses and remove them. Updates are available as free down loads on our mirror download. This page allows you to configure WebScan for Linux to connect automatically to such sites and download updates.

Screen elements are explained as below:

[Update VIRUS Definition Databases](#)

Click the link to immediately download the latest updates. A new update window is opened and you can see the download progress.

[Auto Update Databases](#)

Set a schedule so that WebScan for Linux, downloads updates at a fixed time.

[Auto Update Schedule Time](#)

The two spin boxes allow you to set the time in hours and minutes at which updates are automatically downloaded daily.

[Send Update Notification To](#)

After updates are downloaded, a notification is sent to the ID that you enter here.

[List of Update Servers](#)

A list of MicroWorld mirror download URLs is displayed in the box. Updates are downloaded on a round-robin basis from them. Add or modify the list if required.

[Activate Changes](#)

After entering appropriate values in the above fields, click the button to activate them. A message is displayed in the top row giving status of your changes and warns you if invalid entries are made.

Reset

Clears recent changes made before you have activated the changes

HTTP/FTP Proxy Server for Updates

Select the check box if you use an HTTP/FTP Proxy Server to download updates.

Proxy Address: Enter the IP of the proxy server

Proxy Port: Enter the port number

Proxy Server Authentication Info

Select the check box if authentication is needed to connect to the proxy.

Username: Enter the user name used for login

Password: Enter the password to be used for authentication

Activate Changes

After entering appropriate values in the above fields, click the button to activate them. A message is displayed in the top row giving status of your changes and warns you if invalid entries are made.

Reset

Clears recent changes made before you have activated the changes

Server Logs

This section allows you to view violation logs, WebScan logs and operations logs.

Server Logs Violation Logs

This page provides a log of violations that are logged by WebScan. When users visit banned sites or sites that have offensive content, as per the security policy, such sites are blocked. Details like the client IP that has accessed the URL, the blocked URL, date and time when the activity occurred and the reason why the site was blocked are displayed in the table.

Screen elements are explained as below:

Date and Time

Date and time when the violation occurred is displayed

Client IP

IP of the machine from which the violation occurred is displayed

URL

URL of the offensive site is displayed

Reason

Reason why the site was blocked or recorded as a violation is displayed

Server Logs WebScan Logs

This page provides a log of WebScan activity. You can set the WebScan log size in MB.

Screen elements are explained as below:

WebScan Log file Size in MB

Allows you to specify the WebScan Log File Size in MB.

Activate Changes

After entering appropriate values in the above fields, click the button to activate them. A message is displayed in the top row giving status of your changes and warns you if invalid entries are made.

Reset

Clears recent changes made before you have activated the changes

Refresh

Log details are displayed in the box. Click Refresh to bring up fresh values.

Clear Logs

Entries in the log, shown in the box are cleared

Server Logs WebScan Operations Logs

This page provides a log of WebScan activity. In your WebScan network, you can see a list of IPs and URLs that are accessed along with the date and time when this activity occurred.

Date

Date when the URL and IP was accessed is displayed

Time

Time when the URL and IP was accessed is displayed

Client IP

IP of the machine from which the violation occurred is displayed

URL

URL of the offensive site is displayed

Help

About

Provides version details of WebScan for Linux running on your system, last update downloaded date and the number of virus signatures that are known.

Enter License Key:

The license key allows you to run WebScan for Linux. You can enter a new license key.

Register Product:

You need to register your product after entering the correct license key. If a wrong key is entered then an error message is displayed and you need to enter the correct key

Contacts

Gives our [Contact Information](#)

Help Index

Explains [Key features](#) of WebScan and also gives shortcuts to access the menus