



webwasher®

USER'S GUIDE

Webwasher SSL Scanner
Version 6.0

Part Number: 86-0946227-B

All Rights Reserved, Published and Printed in Germany

©2006 Secure Computing Corporation. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Secure Computing Corporation. Every effort has been made to ensure the accuracy of this manual. However, Secure Computing Corporation makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Secure Computing Corporation shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this document is subject to change without notice. Webwasher, MethodMix, AV PreScan, Live Reporting, Content Reporter, ContentReporter, Real-Time Classifier are all trademarks or registered trademarks of Secure Computing Corporation in Germany and/or other countries. Microsoft, Windows NT, Windows 2000 are registered trademarks of Microsoft Corporation in the United States and/or other countries. McAfee is a business unit of Network Associates, Inc. CheckPoint, OPSEC, and FireWall-1 are trademarks or registered trademarks of CheckPoint Software Technologies Ltd. or its affiliates. Sun and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Squid is copyrighted by the University of California, San Diego. Squid uses some code developed by others. Squid is Free Software, licensed under the terms of the GNU General Public License. The Mozilla SpiderMonkey and NSPR libraries distributed with Webwasher are built from the original Mozilla source code, without modifications (MPL section 1.9). The source code is available under the terms of the Mozilla Public License, Version 1.1. NetCache is a registered trademark of Network Appliances, Inc. in the United States and other countries. Linux is a registered trademark of Linus Torvalds. Other product names mentioned in this guide may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Secure Computing Corporation
Webwasher – A Secure Computing Brand
Vattmannstrasse 3, 33100 Paderborn, Germany
Phone: +49 (0) 5251 50054-0
Fax: +49 (0) 5251 50054-11

info@webwasher.com
www.webwasher.com
www.securecomputing.com

European Hotline
Phone: +49 (0) 5251 50054-460
US Hotline
Phone: +1 800 700 8328, +1 651 628 1500

Contents

Chapter 1 Introduction	1- 1
1.1 About This Guide	1- 2
1.2 What Else Will You Find in This Introduction?	1- 2
1.3 Using Webwasher	1- 3
1.3.1 First Level Tabs	1- 4
1.3.2 Configuring a Sample Setting	1- 5
1.3.3 General Features of the Web Interface	1- 7
1.4 Other Documents	1-11
1.4.1 Documentation on Main Products	1-12
1.4.2 Documentation on Special Products	1-13
1.5 The Webwasher Product Suite	1-14
Chapter 2 Home	2- 1
2.1 Overview	2- 2
2.2 Overview (Feature)	2- 2
2.2.1 Overview (Feature)	2- 3
2.3 Support	2- 7
2.3.1 Support	2- 7
2.4 Feedback	2- 9
2.4.1 Feedback	2-10
2.4.2 Feedback Queues	2-11
2.4.3 Malware Feedback Black List	2-16
2.5 Manuals	2-18
2.5.1 Documentation on Main Products	2-19
2.5.2 Documentation on Special Products	2-21
2.5.3 Additional Documentation	2-23
2.6 Preferences	2-24
2.6.1 Preferences	2-24
2.7 License	2-28
2.7.1 Information	2-29
2.7.2 Notification	2-32
Chapter 3 Common	3- 1
3.1 Overview	3- 2
3.2 Media Type Filters	3- 2
3.2.1 Actions	3- 3
3.2.2 Media Type Black List	3- 7
3.2.3 Media Type White List	3-10
3.3 Document Inspector	3-13
3.3.1 Document Inspector	3-14
3.4 Archive Handler	3-19
3.4.1 Archive Handler	3-20
3.5 Generic Header Filter	3-22
3.5.1 Generic Header Filter	3-23

3.6	Generic Body Filter	3-25
3.6.1	Generic Body Filter	3-26
3.7	Advertising Filters	3-28
3.7.1	Settings	3-29
3.7.2	Link Filter List	3-37
3.7.3	Dimension Filter List.....	3-40
3.8	Privacy Filters	3-43
3.8.1	Settings	3-44
3.8.2	Cookie Filter List.....	3-49
3.9	Text Categorization	3-51
3.9.1	Settings	3-52
3.9.2	Categorization List	3-54
3.10	White List.....	3-57
3.10.1	White List.....	3-58
3.11	User Defined Categories	3-62
3.11.1	User Defined Categories	3-62
3.12	Media Type Catalog	3-64
3.12.1	Media Type Catalog	3-65
Chapter 4	SSL Scanner	4- 1
4.1	Overview	4- 2
4.2	Certificate Verification	4- 2
4.2.1	Certificate Verification	4- 3
4.3	Scan Encrypted Traffic.....	4- 5
4.3.1	Scan Encrypted Traffic.....	4- 6
4.4	Certificate List	4-10
4.4.1	Certificate List	4-11
4.5	Trusted Certificate Authorities.....	4-14
4.5.1	Trusted Certificate Authorities.....	4-15
4.6	Global Certificate List	4-19
4.6.1	Global Certificate List	4-19
4.7	Global Trusted Certificate Authorities	4-23
4.7.1	Global Trusted Certificate Authorities	4-23
4.8	Incident Manager.....	4-25
4.8.1	Incident Manager.....	4-26

Introduction

Welcome to the Webwasher® User's Guide SSL Scanner. It provides you with the information needed to configure and use the SSL Scanner, which is one of the products of the Webwasher Secure Content Management (SCM) Suite.

The Webwasher SSL Scanner enables you to extend your existing security and Internet usage policies to the HTTPS protocol and to prevent certificate misuse.

SSL-encrypted content, including viruses, spyware, MP3s, pornography, and confidential company files, is beyond the reach of any Anti-Virus scanner and content filter.

The SSL Scanner allows you to manage this encrypted content in the same way as HTTP content and thus to prevent policy evasion, while it is also scanning Web traffic for all kinds of threats to your network.

1.1

About This Guide

The following overview lists the chapters of this guide and explains briefly what they are about:

User's Guide SSL Scanner	
Introduction	Provides introductory information.
Home	Describes basic features that are common to the SSL Scanner and other Webwasher products.
Common	Describes filtering features that are common to the SSL Scanner and other Webwasher products.
SSL Scanner	Describes the filtering features that are specific to the SSL Scanner.

1.2

What Else Will You Find in This Introduction?

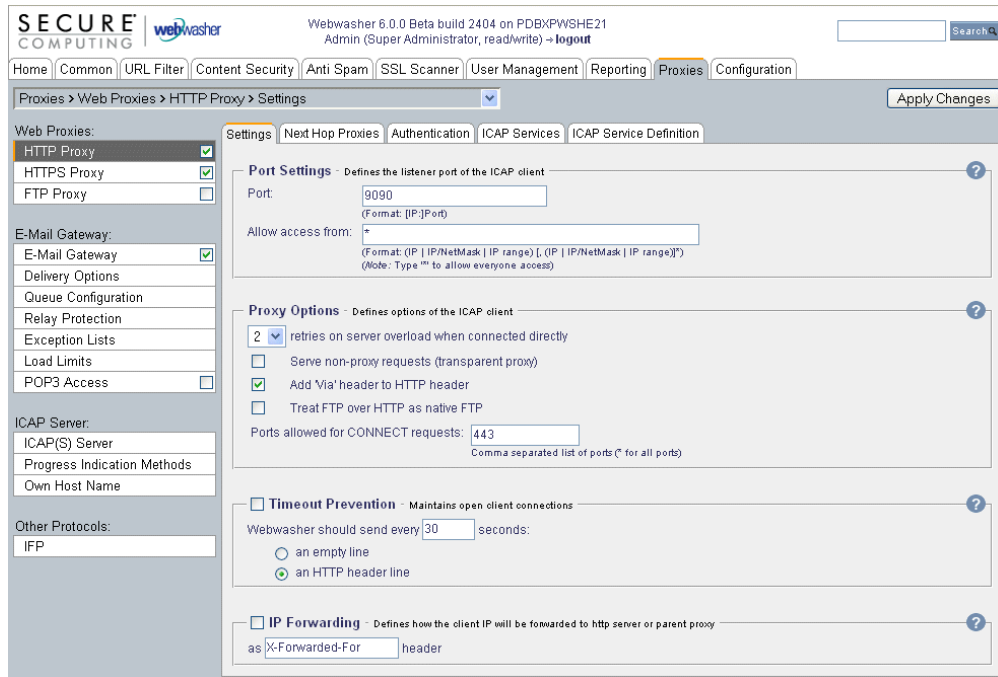
In addition to the overview that was given in the previous section, this introduction also:

- Explains how to handle the Web interface that is provided for using Webwasher, see [1.3](#).
- Informs you about the other documents that are provided for users of Webwasher, see [1.4](#).
- Describes briefly the products that make up the Webwasher product suite, see [1.5](#).

1.3

Using Webwasher

A user-friendly, task-oriented Web interface has been designed for accessing the features of the Webwasher products. It looks like this:



The following sections provide information to make you familiar with the way this interface is used. These sections:

- List the first level tabs of this interface and explain their meanings, see [1.3.1](#).
- Describe a sample procedure showing how a setting is configured for a Webwasher feature, see [1.3.2](#).
- Explain general features of this interface, see [1.3.3](#).

1.3.1 First Level Tabs

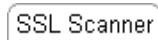
The Web interface displays a number of tabs and sections for configuring the features provided by Webwasher. On the topmost level, there are these tabs:

- Home, Common, URL Filter, Content Security, Anti Spam, SSL Scanner, User Management, Reporting, Proxies, and Configuration

Their meaning is as follows:

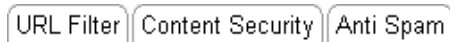


Home, Common – These tabs are for configuring basic and filtering features that are used not only by the SSL Scanner, but also by other Webwasher products. Among these features are, e. g. system alerts, licensing features, media type filters, etc.



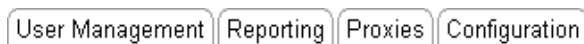
SSL Scanner – This is the top level tab for configuring the features that are specific to the SSL Scanner.

The tabs mentioned in the following are not described in this guide:



URL Filter, Content Security, Anti Spam – These tabs are for configuring the features of other Webwasher products. Note that the *Content Security* tab is used for the Anti-Virus, Anti-Malware and Content Protection products.

For a description of these tabs, see the corresponding User's Guides.



User Management, Reporting, Proxies, Configuration – These are tabs for configuring features that adapt Webwasher to the system environment it is running in.

For their description, see the System Configuration Guide.

1.3.2 Configuring a Sample Setting

This section explains how to configure a sample setting of a Webwasher feature. The feature chosen here for explanation is the *Animation Filter*.

In order to avoid the download of bandwidth-consuming animated images, this filter detects and modifies or removes them.

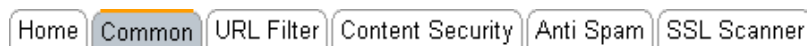
For this sample setting, just suppose you want to enable the filter and let it remove any such images from the filtered objects. You also want these settings to be part of your default filtering policy.

The following overview shows the main steps you need to complete in order to configure the feature in this way:

Animation Filter – Overview	
Step 1	Navigate to the section.
2	Configure settings.
3	Make settings effective.

In more detail, these steps include the following activities:

1. *Navigate to the section*
 - a. Select the *Common* tab:



- b. In the navigation area on the left, select *Advertising Filters*, which is located under *Policy*:

Policy:	
default	<input type="checkbox"/>
Media Type Filters	<input type="checkbox"/>
Document Inspector	<input checked="" type="checkbox"/>
Archive Handler	<input checked="" type="checkbox"/>
Generic Header Filter	<input checked="" type="checkbox"/>
Generic Body Filter	<input checked="" type="checkbox"/>
Advertising Filters	<input checked="" type="checkbox"/>
Privacy Filters	<input type="checkbox"/>
Text Categorization	<input type="checkbox"/>
White List	<input type="checkbox"/>

default is selected in the line below *Policy*. Since you want these settings to be part of your default filtering policy, you can leave this selection as it is.

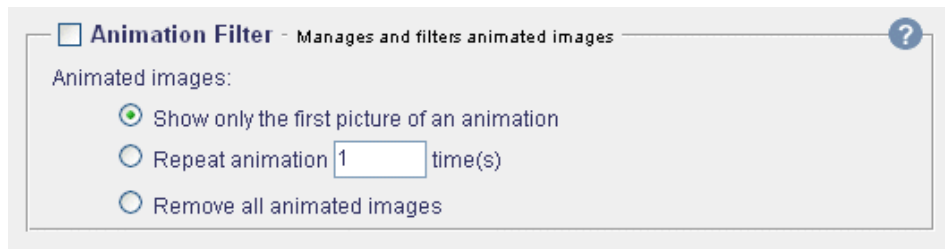
Otherwise, you could select a different filtering policy, using the drop-down list.

As you will have noticed, *Advertising Filter* is enabled, which is the default setting for this feature, so you can also leave it as it is.

c. From the tabs provided for configuring the *Advertising Filters* options, select the *Settings* tab:



The *Animation Filter* section is located on this tab:



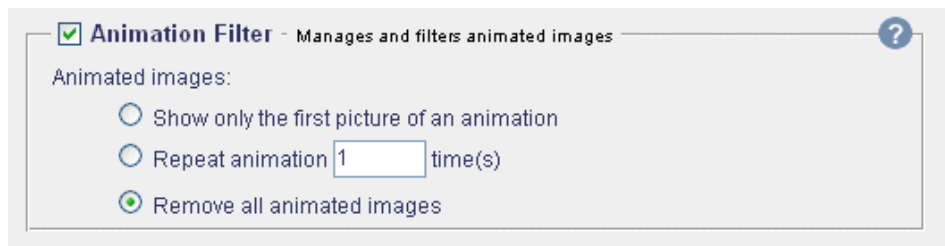
2. *Configure settings*

a. Enable the feature. To do this, mark the checkbox next to the section heading.

b. Check the radio button labeled *Remove all animated images*.

Note: To get help information about these settings, click on the question mark in the top right corner of the section.

The section should now look like this:



3. *Make settings effective*

Click on the *Apply Changes* button:



1.3.3 General Features of the Web Interface

This section explains a number of features that are provided in the Web interface for solving general tasks, e. g. applying changes to the Webwasher settings or searching for a term on the tabs of the interface.

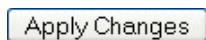
The following features are explained here:

- *Apply Changes*
- *Click History*
- *Information Update*
- *Logout*
- *Main Feature Enabling*
- *Search*
- *Session Length*
- *System Information*


Apply Changes

After modifying the settings in one or more of the sections on a tab, you need to click on the *Apply Changes* button to make effective what you have modified.

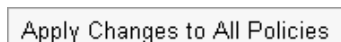
The *Apply Changes* button is located in the top right corner of the Web interface area:

A rectangular button with a thin border and the text "Apply Changes" inside.

When modifying settings that belong only to a particular filtering policy, you can make the modified settings apply to all policies nevertheless. An arrow is displayed next to the *Apply Changes* button on each tab where policy-dependent settings can be configured.

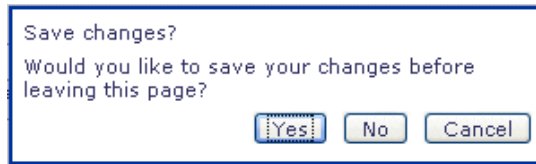
A rectangular button with a thin border, the text "Apply Changes", and a small downward-pointing triangle (dropdown arrow) to its right.

Clicking on this arrow will display a button, which you can use to apply changes to all policies.

A rectangular button with a thin border and the text "Apply Changes to All Policies" inside.

After clicking on this button, your modifications will be valid for settings of all policies.

When you are attempting to leave a tab after modifying its settings, but without clicking on *Apply Changes*, an alert is displayed to remind you to save your changes:



Answer the alert by clicking *Yes* or *No* according to what you intend to do about your changes. This will take you to the tab you invoked before the alert was displayed.

Clicking on *Cancel* will make the alert disappear, so you can continue your configuration activities on the current tab.

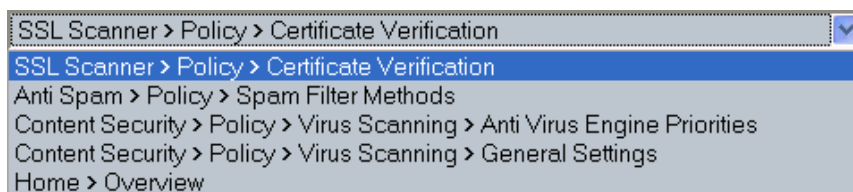
Click History

The tabs you visited while configuring settings are recorded on the top left corner of the Web interface area. They are recorded together with the paths leading to them.

The current tab and path are always visible in the display field, e. g.:



Clicking on the arrow to the right of the path display will show the “click history”, i. e. a list of the tabs you visited prior to this one:



Clicking on any of the entries displayed in the list will take you to the corresponding tab.

The click history is only recorded for the current session, i. e. until you log out. After logging in for a new session, the recording of tabs and paths will start all over again.

Information Update

Some parts of the information that is provided on the tabs of the Web interface will change from time to time. In these cases, the information display is updated automatically every three seconds by Webwasher.

So, e. g. you might have performed a manual update of the anti-virus engines. This means that the information provided in the *Current Status* and *Log File Content* sections on the corresponding *AV Engine* tab will begin to change continuously over a certain period of time until the update is completed.

These sections are then updated automatically every three seconds to reflect the status of the update process.

Logout


To logout from a Webwasher session, click on the *logout* link, which is located in middle position at the top of the Web interface area.

After logging out, the login page is displayed, where you can login again and start a new session.

Main Feature Enabling

There are Webwasher settings that cannot only be modified if a corresponding main feature is disabled. So, e. g. if you want to modify the settings of the *Phishing Filter* section on the *Settings* tab under *Anti-Spam > Message Filters*, you need to make sure the *Message Filter* feature itself is also enabled.

If you attempt to modify settings where the corresponding main feature is not enabled, an alert is displayed to make you aware of this situation:

 Your changes will have no effect, because the main feature is disabled

Search

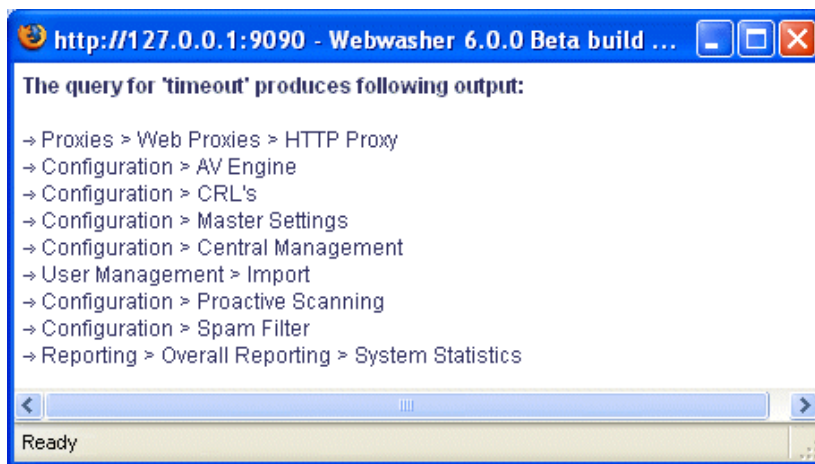
A *Search* input field and button are located in the top right corner of the Web interface area.



Using these, you can start keyword queries of the entire Web interface by entering a search term in the input field and clicking on the *Search* button:



The search output will be presented in a separate window, which displays a list of the tabs the search term was found on and the paths leading to them:



Clicking on any of the entries displayed in the list will take you to the corresponding tab.

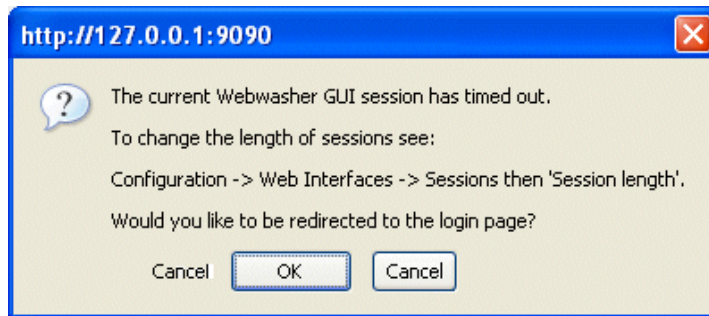
Note: In order to be able to use the search function, make sure JavaScript is enabled.

Session Length

When working with the Web interface, you need to mind the session length.

This interval can be configured in the *Session Options* section of the *Sessions* tab under *Configuration > Web Interfaces*.

After modifying the interval specified there, click on *Apply Changes* to make this setting effective.



Clicking *OK* will redirect you to the login page, where you can login again and start a new session.

System Information

At the top of the Web interface area, system information is provided on the current Webwasher session. This information includes:

- Version and build of the Webwasher software
- Name of the system Webwasher is running on
- Name of the user logged in for the current session, e. g. *Admin*
- Role assigned to this user, e. g. *Super Administrator*
- Permission granted to this user, e. g. *read/write*

1.4 Other Documents

This guide belongs to a series of documents provided for users of Webwasher. The following sections give an overview of them.

The Webwasher user documentation can be viewed after navigating to the *Manuals* tab of the Web interface.

It can also be viewed in the Webwasher Extranet (Resource Center).

The following is provided:

- Documentation on the main products of Webwasher, see [1.4.1](#)
- Documentation on products for special tasks and environments, see [1.4.2](#)

1.4.1 Documentation on Main Products

This section introduces the user documentation on the main products of Webwasher.

Document Group	Document Name	What about?
General Documents	Deployment Planning Guide	Is Webwasher suited to my environment?
	Installation Guide	How to install Webwasher?
	Quick Configuration Guide	First steps to get Webwasher running.
	System Configuration Guide	Features for configuring Webwasher within the system environment.
	Advanced Configuration Guide	More sophisticated configuration tasks.
	Upgrade Guide	What should I know when upgrading to a new Webwasher release?
Product Documents	User's Guide URL Filter	Features for configuring URL filtering policies.
	User's Guide Anti-Virus	Features for configuring anti-virus filtering policies.
	User's Guide Anti-Malware	Features for configuring anti-malware filtering policies.
	User's Guide Content Protection	Features for configuring content protection filtering policies.
	User's Guide Anti-Spam	Features for configuring spam filtering policies.
	User's Guide SSL Scanner – <i>this document</i>	Features for configuring SSL-encrypted traffic filtering policies.
Reference Document	Reference Guide	Items concerning more than product, e. g. features for customizing actions or log files.

1.4.2 Documentation on Special Products

This section introduces the user documentation on products for special tasks and environments.

Document Group	Document Name	What about?
Content Reporter Documents	Content Reporter Installation and Configuration Guide	Installing and configuring the Webwasher Content Reporter, which is done separately from the main products.
	Content Reporter User's Guide for Reporting	Creating reports.
Instant Message Filter Documents	Instant Message Filter Installation and Configuration Guide	Installing and configuring the Webwasher Instant Message Filter, which is done separately from the main products.
	User's Guide Instant Message Filter	Description of features.
Special Environment Documents	Setting Up Webwasher on Microsoft ISA Server	Setting up Webwasher or a product running with it in a special environment.
	Setting Up Webwasher with Blue Coat	See above.
	Setting Up NetCache with ICAP	See above.
	NTLM Agent Set-up Guide	Setting up an additional Webwasher product to enable authentication using the NTLM method on platforms other than Windows.
	HSM Agent Set-up Guide	Setting up an additional Webwasher product to enable use of a HSM (High Security Module) device.
Appliance Documents	Appliance Installation and Configuration Guide	Installing and configuring the Webwasher appliances.
	Appliance Upgrade Guide	What should I know when upgrading to a new release of the Webwasher appliances?







1.5

The Webwasher Product Suite

The Webwasher suite of products provides an optimal solution for all your secure content management needs.



It is unique in that it offers best-of-breed security solutions for individual threats and at the same time a fully integrated architecture that affords in-depth security and cost/time savings through inter-operability.

The following products are included in this suite:

	Webwasher® URL Filter	Helps you boost productivity by reducing non-business related surfing to a minimum, thus curbing your IT costs. Suppresses offensive sites and prevents downloads of inappropriate files, thus minimizing risks of legal liabilities.
	Webwasher® Anti-Virus	Combines the strength of multiple anti-virus engines concurrently scanning all Web and e-mail traffic. The Proactive Scanning filtering technology additionally detects and blocks unknown malicious code, not relying on time-delayed virus pattern updates. This combination provides in-depth security against a multitude of threats while offering unmatched performance through use of the Anti-Virus PreScan technology.
	Webwasher® Anti-Malware	Offers in-depth security against all kinds of malicious code, such as aggressive viruses, potentially unwanted programs, spyware, day-zero attacks and blended threats not covered by traditional anti-virus and firewall solutions. The highly efficient anti-malware engine is used in combination with the Proactive Scanning filtering technology.
	Webwasher® Content Protection	Ensures that your systems are protected against myriads of threats transported in Web and e-mail traffic. In addition to applying the Proactive Scanning filtering technology, outbound filters stop leakage of company-sensitive data and prevent identity theft.
	Webwasher® Anti-Spam	Offers complete protection of the central Internet gateway. The highly accurate spam detection filters stem the flood of unwanted spam mail before it reaches the user's desktop. Your systems will not be impaired, the availability of valuable internal mail infrastructures, such as group servers, is thus maintained.
	Webwasher® SSL Scanner	Helps you protect your network against attacks via the HTTPS protocol and prevents the disclosure of confidential corporate data, as well as infringements of Internet usage policies, thus ensuring that no one is illicitly sharing sensitive corporate materials.

See next page

The following two products have their own user interfaces, which are described in the corresponding guides, see also [1.4.2](#).

	Webwasher® Content Reporter	Features a library of rich, customizable reports based on built-in cache, streaming media, e-mail activity, Internet access and content filtering queries, all supported by unmatched convenience and performance features.
	Webwasher® Instant Message Filter	Detects, reports and selectively blocks the unauthorized use of high-risk and evasive P2P and IM from enterprise networks and scans network traffic for characteristics that match the corresponding protocol signatures.

Home

The features that are described in this chapter are accessible over the *Home* tab of the Web interface:

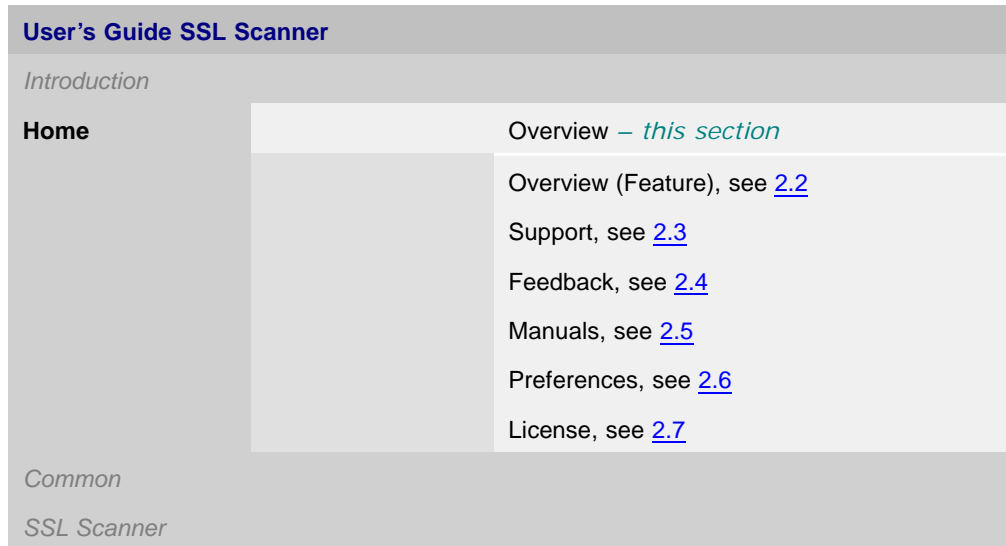


These are basic features that are common to the SSL Scanner and other Web-washer products, e. g. system alerts, contacting the support, licensing features, etc.

The upcoming sections describe how to handle these features. The description begins with an overview.

2.1 Overview

The following overview shows the sections that are in this chapter:

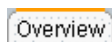


2.2 Overview (Feature)

The *Overview* options are invoked by clicking on the corresponding button under *Home*:



The options are arranged under the following tab:



They are described in the upcoming section:

- *Overview (Feature)*, see [2.2.1](#)

2.2.1 Overview (Feature)

The *Overview* tab looks like this:

System Alerts - Displays important system warnings and messages

- The default root certificate is used by SSL Scanner. In order to avoid security problems → **create your own certificate.**
- There has been no Anti Virus update check for at least 3 days. → **Check Update Manager**
- Spam Filter method "Real-Time Blackhole Lists" cannot operate without further setup. → **Setup RBL filter.**
- Email server for notification delivery is not defined. → **Define server and sender.**
- Recipient for system notifications is not set. → **Enter email address.**
- Anti Virus engines order is not defined. The system will scan the object using the default engines order. → **Set AV engine priorities.**
- Recipient for Virus email notifications is not set. → **Enter email address.**

System Summary - Displays the latest system modifications and updates

System Settings	Admin	Tue Aug 29 17:00:06 2006
Current Policy (default)	Admin	Tue Aug 29 17:02:30 2006
→ URL Filter Database	Database Number: 1509	Tue Aug 29 16:56:27 2006
→ Anti Virus Engine and Signatures	Computer Associates - ETrust Inoculate IT 23.72.35 (2006-6-13) McAfee Antivirus - Engine '5.0.00', Rev 5000.741, DAT Version 4782 Sophos 2381-4.06 (123312 viruses)	Tue Jun 13 10:58:41 2006
→ Spam Filter Rules	Database Number: 9954	Tue Aug 29 16:53:14 2006
→ Certificate Revocation Lists		Tue Jun 13 10:59:49 2006
→ Proactive Scanning Database	Database Number: 0	Tue Jun 13 10:57:55 2006

One-Click Lockdown - Use single strict policy ?

Version Information

CSM Suite	6.0.0 Beta
Build Number	2404
Part Number	101-0946150-A
Build Date	Aug 29 2006
Operating System	Windows

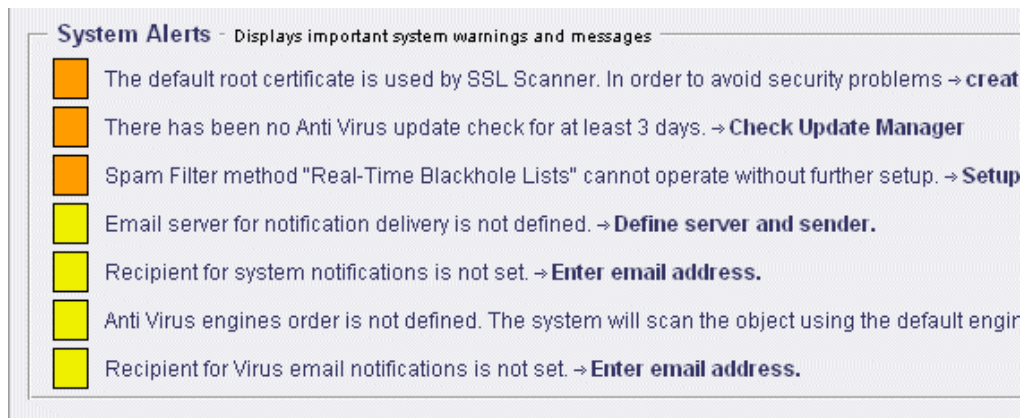
There are four sections on this tab:

- *System Alerts*
- *System Summary*
- *One-Click Lockdown*
- *Version Information*

They are described in the following.

System Alerts

The *System Alerts* section looks like this:



This section displays alerts to make you aware of problems concerning the system status. The function underlying these alerts is also known as "Security Configurator".

To the left of each alert text, a field in red, orange, or yellow color indicates the relative importance of the alert.

To the right of each alert text, a link is displayed. Click on this link to navigate to a tab where you can configure the relevant settings as a measure against the problem that caused the alert.

So, e. g., the warning *There has been no Anti Virus update check for at least 3 days* is followed by a link labeled *Check Update Manager*.

Clicking on that link will take you to the *AV Engine* tab, where an update of the kind requested by the alert can be performed.

An alert is repeated on tab or tabs dealing with the topic in question.

So, e. g. the warning *There has been no Anti Virus update check for at least 3 days*, is repeated on the *General Settings* tab, which is provided for configuring the general settings of virus scanning.

System Summary

The *System Summary* section looks like this:

System Summary - Displays the latest system modifications and updates	
System Settings	Admin
Current Policy (default)	Admin
→ URL Filter Database	Database Number: 1509
→ Anti Virus Engine and Signatures	Secure Anti-Malware - 6035.18.1 Computer Associates - ETrust In (2006-6-13) McAfee Antivirus - Engine '5.0.00 Version 4782 Sophos 2381-4.06 (123312 virus
→ Spam Filter Rules	Database Number: 9954
→ Certificate Revocation Lists	
→ Proactive Scanning Database	Database Number: 0

This section displays information on the system status.

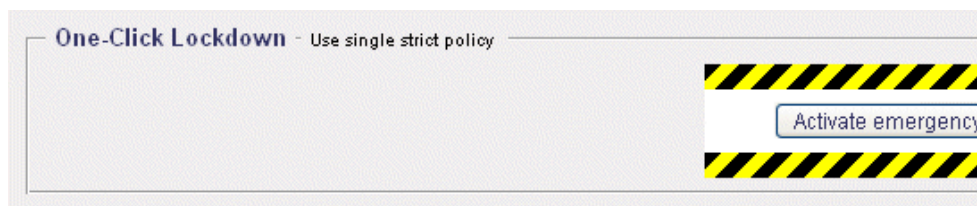
Information is provided on the user who is currently logged in and on the anti virus engines that are installed showing also their current versions.

Furthermore, the last updates of the databases containing the rules for filtering URLs, viruses and spam are displayed, as well as the version of the certificate revocation list.

Clicking on the links that are provided here, e. g. on the *Proactive Scanning Database* link, will take you to the corresponding *Update Manager* tabs, where you can configure and manually perform updates of the databases.

One-Click Lockdown

The *One-Click Lockdown* section looks like this:



Using this section, you can enable an emergency mode to apply a single strict policy overruling all other policies.

This might be useful in a situation when, e. g. a new virus emerges. You may then want to replace all policies that were configured for different users and user groups by one single policy, which is rather strict and binding for all.

To enable the emergency mode:

- Click on the *Activate emergency mode* button.



This button is a toggle switch. After enabling the emergency mode, the inscription on it will read *Back to normal mode*.

To disable the emergency mode:

- Click on the *Back to normal mode* button.



When the emergency mode is enabled, there is also an alert in the *System Alerts* section of this tab to remind you it is enabled:



It is recommended to turn the emergency mode off when it is no longer needed.

To select the policy that will be used under the emergency mode, go to the *Mapping Process* section on the *Web Mapping* tab under *User Management > Policy Management*.

The default policy to be applied under the emergency mode is a policy named *Emergency*. You may also retain this policy and its settings or modify them according to your requirements.

Version Information

The *Version Information* section looks like this:



This section displays information on the product version and also some related information, such as the current software build or the operating system Web-washer is running on.

To see if there is a newer version of the software available, click on the *Check for New Versions* button.

2.3 Support

The *Support* options are invoked by clicking on the corresponding button under *Home*:

Support

The options are arranged under the following tab:

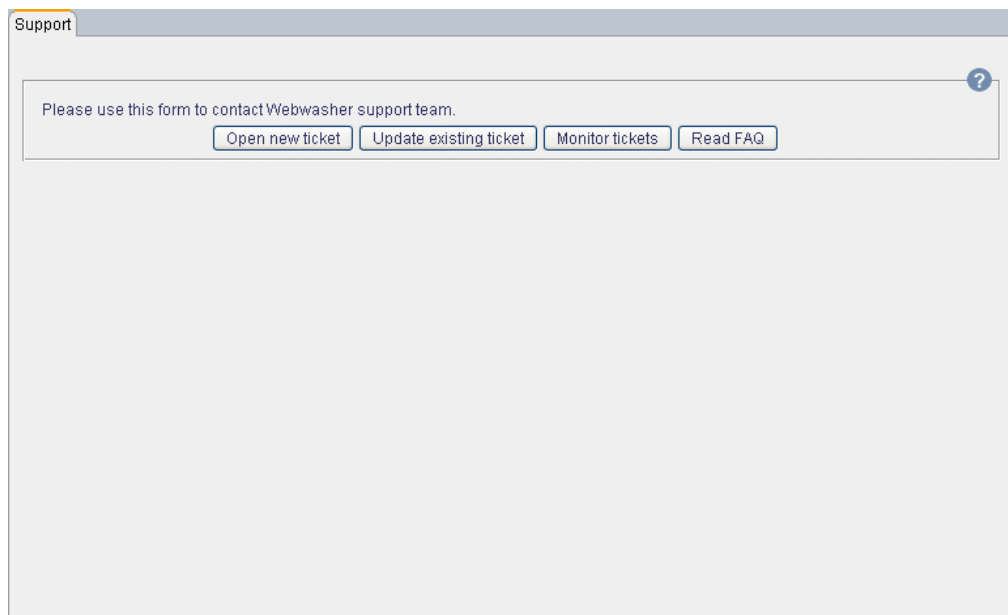
Support

They are described in the upcoming section:

- *Support*, see [2.3.1](#)

2.3.1 Support

The *Support* tab looks like this:



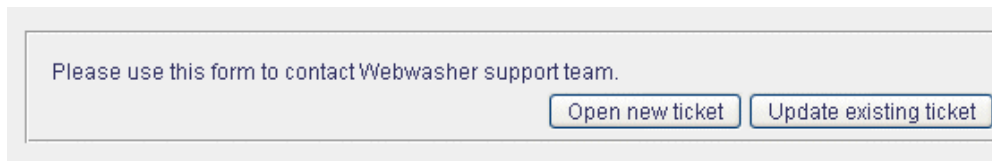
There is one section on this tab:

- *Support*

It is described in the following.

Support

The *Support* section looks like this:



Using this section, you can contact the Webwasher support team.

The section provides a number of buttons. Each of them can be used for a different kind of contact:

- *Open new ticket*

Using this button, you can contact the support to submit a problem concerning Webwasher. After submitting the problem, you receive what is termed a “ticket”, representing the support case that has been opened for you.

Clicking on the button launches a login page. After successfully logging in, you are provided with more information about how to open a new ticket.

- *Update existing ticket*

Using this button, you can update a ticket that has been opened for you before. You can alter the message text belonging to this ticket or modify an attachment that was sent with it. After making your updates, you can resend the ticket.

- *Monitor tickets*

Using this button, you can contact the support to monitor the tickets that were opened for you before.

Clicking on the button launches a login page. After successfully logging in, you are provided with more information about how to monitor tickets.

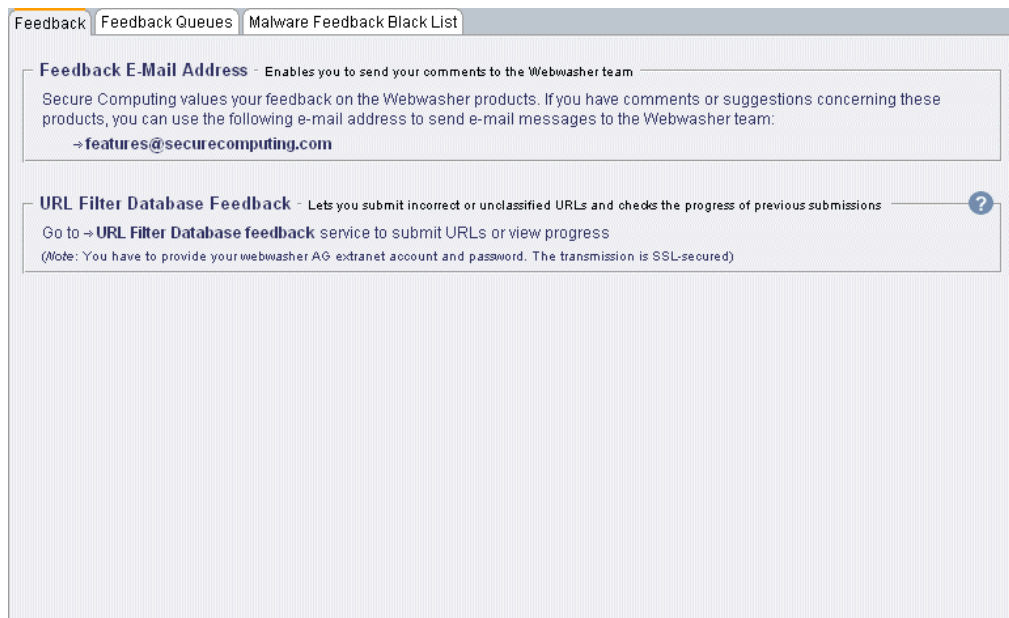
- *Read FAQ*

Using this button, you can contact the support to read Frequently Asked Questions on Webwasher problems.

Clicking on the button launches a login page. After successfully logging in, you are provided with more information about the reading procedure.

2.4 Feedback

The *Feedback* options are invoked by clicking on the corresponding button under *Home*:



The options are arranged under the following tabs:

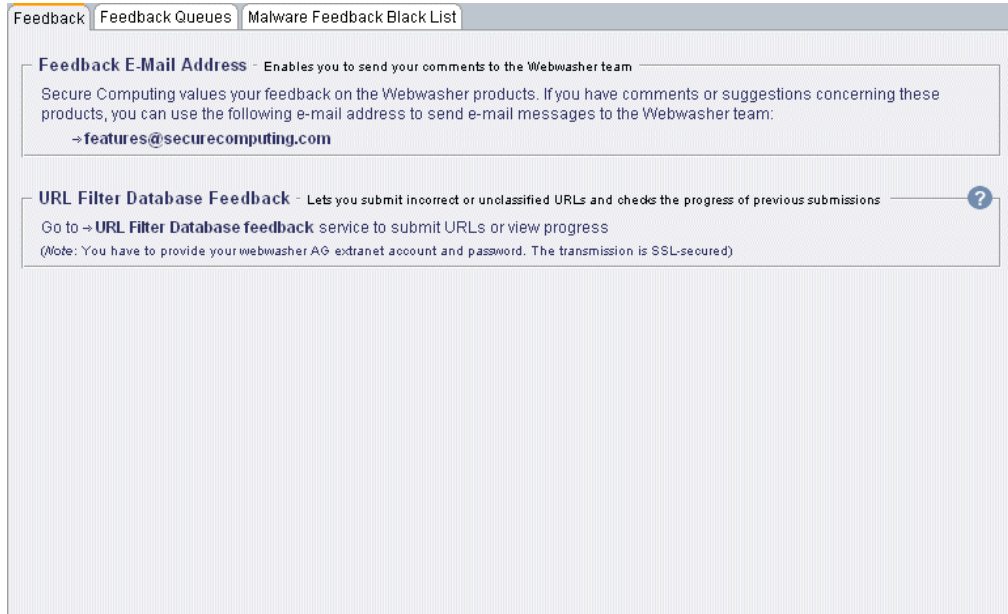


They are described in the upcoming section:

- *Feedback*, see [2.4.1](#)
- *Feedback Queues*, see [2.4.2](#)
- *Malware Feedback Black List*, see [2.4.3](#)

2.4.1 Feedback

The *Feedback* tab looks like this:



There are two sections on this tab:

- *Feedback E-Mail Address*
- *URL Filter Database Feedback*

They are described in the following.

Feedback E-Mail Address

The *Feedback E-Mail Address* section looks like this:



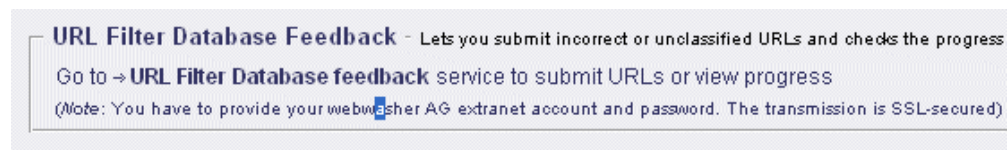
Using this section, you can send feedback concerning the Webwasher products to Secure Computing.

To send your feedback, click on the features@securecomputing.com link provided in this section.

This will open an e-mail message sheet, which you can fill in and send off.

URL Filter Database Feedback

The *URL Filter Database Feedback* section looks like this:



Using this section, you can submit unclassified or incorrectly classified URLs to Secure Computing.

To do this, click on the *URL Filter Database feedback* link provided in this section.

This will launch the login page for accessing the Webwasher Extranet. After successfully logging in there, a *Welcome* page is displayed. On this page, click on the option labeled *Feedback system for URL Filter categorization*.

Then follow the instructions given on the *URL Filter Feedback* page.

2.4.2 Feedback Queues

The *Feedback Queues* tab looks like this:

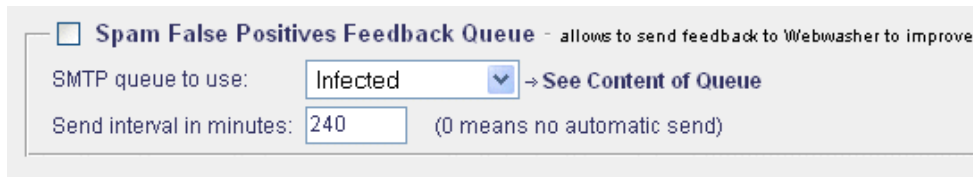
There are three sections on this tab:

- [Spam False Positives Feedback Queue](#)
- [Spam False Negatives Feedback Queue](#)
- [Malware Feedback Queue](#)

They are described in the following.

Spam False Positives Feedback Queue

The [Spam False Positives Feedback Queue](#) section looks like this:



The screenshot shows a configuration panel for the 'Spam False Positives Feedback Queue'. At the top, there is a checkbox and the text 'Spam False Positives Feedback Queue - allows to send feedback to Webwasher to improve'. Below this, there are two main settings: 'SMTP queue to use:' with a dropdown menu currently set to 'Infected' and a link '→ See Content of Queue' to its right; and 'Send interval in minutes:' with an input field containing '240' and a note '(0 means no automatic send)' to its right.

Using this section, you can configure the sending of feedback in order to improve the spam filter.

E-mails that were released from a queue after receiving a digest e-mail will be copied to the false positives queue and sent from there to Secure Computing.

This feature is not enabled by default. If you would like to help improve the spam filter, please mark the checkbox next to the section heading.

After specifying this and other settings of this section, click on [Apply Changes](#) to make your settings effective.

Use the following items to configure the false positives feedback:

- [SMTP queue to use](#)

From this drop-down list, select an e-mail queue. After being released from another queue, e-mails will be copied to this queue and later be sent to Secure Computing.

The queue should be used for no other purpose than that of collecting false positives since it will be cleared after e-mails have been sent off.

To see the e-mails that are in this queue, click on the See Content of Queue link next to the drop-down list.

- [Send interval in . . . minutes](#)

In the input field provided here, enter a time interval (in minutes) to specify the time that is to elapse between sending e-mails.

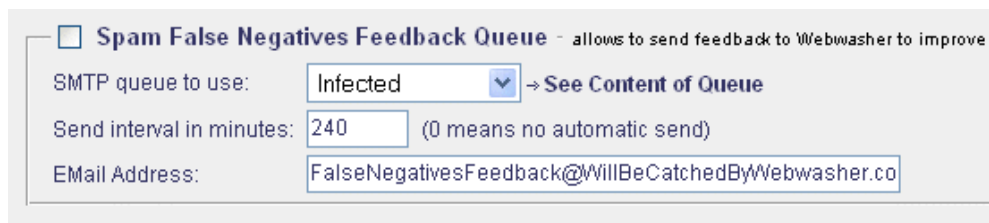
The default interval is 240 minutes. Entering 0 here means that no e-mails will be sent automatically.

E-mails can be sent manually, however, using the [Queue Management](#) page, which is launched after clicking on the [See Content of Queue](#) link next to the drop-down list.

On this page, click on the button labeled [Send All to SecureLabs now](#) to send the e-mails.

Spam False Negatives Feedback Queue

The [Spam False Negatives Feedback Queue](#) section looks like this:



Spam False Negatives Feedback Queue - allows to send feedback to Webwasher to improve

SMTP queue to use: → [See Content of Queue](#)

Send interval in minutes: (0 means no automatic send)

E-Mail Address:

Using this section, you can configure the sending of feedback in order to improve the spam filter.

You can send e-mails that have erroneously not been classified as spam to an address that is configured in this section. After e-mails with this address have been received in the inbound queue of your Webwasher instance, they will be moved from there to the false negatives queue and later be sent to Secure Computing.

This feature is not enabled by default. If you would like to help improve the spam filter, please mark the checkbox next to the section heading.

After specifying this and other settings of this section, click on [Apply Changes](#) to make your settings effective.

Use the following items to configure the false negatives feedback:

- [SMTP queue to use](#)

From this drop-down list, select an e-mail queue. After being received in the inbound queue, an e-mail with the address specified further below will be moved to this queue as false negative and later be sent to Secure Computing.

The queue should be used for no other purpose than that of collecting false negatives since it will be cleared after e-mails have been sent off.

To see the e-mails that are in this queue, click on the [See Content of Queue](#) link next to the drop-down list.

- [Send interval in . . . minutes](#)

In the input field provided here, enter a time interval (in minutes) to specify the time that is to elapse between sending e-mails.

The default interval is 240 minutes. Entering 0 here means that no e-mails will be sent automatically.

E-mails can be sent manually, however, using the [Queue Management](#) page, which is launched after clicking on the [See Content of Queue](#) link next to the drop-down list.

On this page, click on the button labeled [Send All to SecureLabs](#) now to send the e-mails.

- [E-mail address](#)

In this input field, enter an e-mail address. All e-mails received by Webwasher containing this address will be moved to the queue specified above.

The default address is [FalseNegativesFeedback@WillBeCaughtBy-Webwasher.com](#).

Malware Feedback Queue

The [Malware Feedback Queue](#) section looks like this:



Using this section, you can configure the sending of feedback in order to improve the malware filter.

An e-mail that was classified as spam and contains an attachment where no virus was found, will be copied to the malware queue and later be sent to Secure Computing. Small downloads will also be copied to this queue if at least one of the Anti Virus engines or the Proactive Scanning filter detected a virus, but not all engines came to the same result.

This feature is not enabled by default. If you would like to help improve the malware filter, please mark the checkbox next to the section heading.

After specifying this and other settings of this section, click on [Apply Changes](#) to make your settings effective.

Use the following items to configure the malware feedback:

- *SMTP queue to use*

From this drop-down list, select an e-mail queue. E-mails and small downloads matching the criteria explained above will be moved to this queue as malware and later be sent to Secure Computing.

The queue should be used for no other purpose than that of collecting malware since it will be cleared after e-mails and downloads have been sent off.

To see the e-mails that are in this queue, click on the [See Content of Queue](#) link next to the drop-down list.

- *Send interval in . . . minutes*

In the input field provided here, enter a time interval (in minutes) to specify the time that is to elapse between sending e-mails.

The default interval is 240 minutes. Entering 0 here means that no e-mails will be sent automatically.

E-mails can be sent manually, however, using the [Queue Management](#) page, which is launched after clicking on the [See Content of Queue](#) link next to the drop-down list.

On this page, click on the button labeled [Send All to SecureLabs now](#) to send the e-mails.

2.4.3 Malware Feedback Black List

The *Malware Feedback Black List* tab looks like this:

The screenshot shows a web interface with three tabs: 'Feedback', 'Feedback Queues', and 'Malware Feedback Black List'. The active tab is titled 'Malware Feedback Media Type Black List - Defines malware media types that should not be put to the feedback queue'. Below the title, there is a form with a dropdown menu for 'Select media type from catalog:' containing 'application/ace', a text input for 'Description:' with the placeholder '<Enter description here>', and an 'Add to Malware Feedback Media Type Black List' button. Below this form, it says 'Found 1 entries with **' and 'Number of entries per page: 10'. A table with columns 'Select', 'Media Type', and 'Description' contains one entry: 'application/ace' with description '<Enter description here>'. To the right of the table are checkboxes for 'Ignore in media type filter' and 'Ignore in web upload filter'. At the bottom of the table area are 'Select All' and 'Delete Selected' buttons.

There is one section on this tab:

- *Malware Feedback Media Type Black List*

It is described in the following.

Malware Feedback Media Type Black List

The *Malware Feedback Media Type Black List* section looks like this:

This is a close-up of the section shown in the previous screenshot. It features the same title and form for adding a new entry. The table below shows the single entry 'application/ace' with its description. The 'Ignore in media type filter' and 'Ignore in web upload filter' checkboxes are visible to the right of the table row. The 'Select All' and 'Delete Selected' buttons are at the bottom of the table area.

Using this section, you can add a media type to the Media Type Black List for malware feedback. Objects belonging to the media types on this list will not be entered in the malware feedback queue.

To add a media type to the black list, use the area labeled:

- *Select media type from catalog*

Select the media type you want to have blacklisted from the drop-down list provided here, e. g. *application/ace*.

Furthermore, use the following items when adding a media type:

- *Description*

Input in this field is optional. You may enter a description of the media type here.

- *Add to Malware Feedback Media Type Black List*

After selecting a media type, click on this button to add it to the list.

The Feedback Media Type Black List is displayed at the bottom of this section.

To display only a particular number of list entries at a time, type this number in the input field labeled *Number of entries per page* and enter it using the *Enter* key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To sort the list in ascending or descending order, click on the symbol next to the *Media Type* or *Description* column heading.

To edit an entry, type the appropriate text in the input field of the *Description* column and enable or disable the following options:

- *Ignore in media type filter*

If this option is enabled the media type in question will be ignored when the Media Type Filter is applied to Web and e-mail downloads.

- *Ignore ignore in web upload filter*

If this option is enabled the media type in question will be ignored when the Web Upload Filter is applied to outbound user-originating files via HTTP, HTTPS and FTP.

Then click on *Apply Changes* to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- *Filter*

Type a filter expression in the input field of the *Media Type* or *Description* column or in both and enter this using the *Enter* key of your keyboard. The list will then display only entries matching the filter.

- *Delete Selected*

Select the entry you wish to delete by marking the *Select* checkbox next to it and click on this button. You can delete more than one entry in one go.

To delete all entries, mark the *Select all* checkbox and click on this button.

2.5 Manuals

The *Manuals* options are invoked by clicking on the corresponding button under *Home*:

The options are arranged under the following tabs:

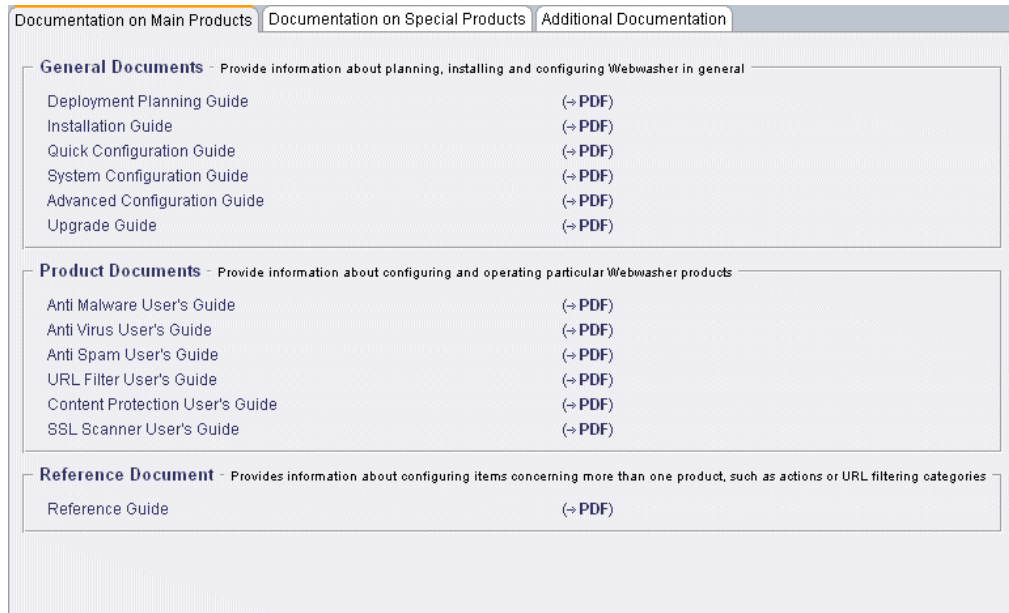
Documentation on Main Products	Documentation on Special Products	Additional Documentation
--------------------------------	-----------------------------------	--------------------------

They are described in the upcoming sections:

- *Documentation on Main Products*, see [2.5.1](#)
- *Documentation on Special Products*, see [2.5.2](#)
- *Additional Documentation*, see [2.5.3](#)

2.5.1 Documentation on Main Products

The *Documentation on Main Products* tab looks like this:



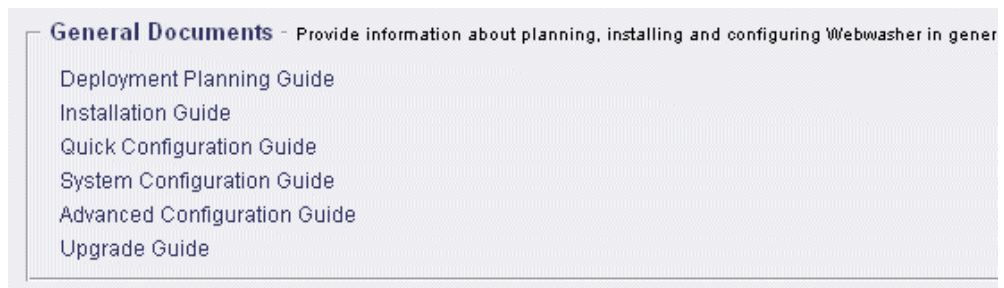
There are three sections on this tab:

- *General Documents*
- *Product Documents*
- *Reference Document*

They are described in the following.

General Documents

The *General Documents* section looks like this:

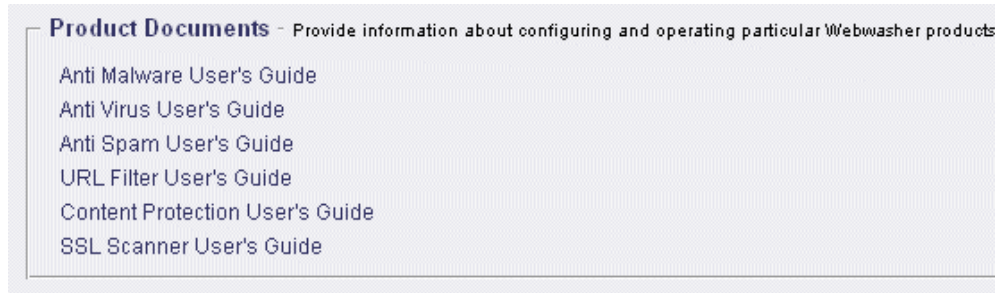


This section allows you to view user documentation on planning, installing and configuring Webwasher in general.

To view any of the documents listed here, click on the [PDF](#) link in the same line. This will open a [.pdf](#) format version of the document.

Product Documents

The [Product Documents](#) section looks like this:

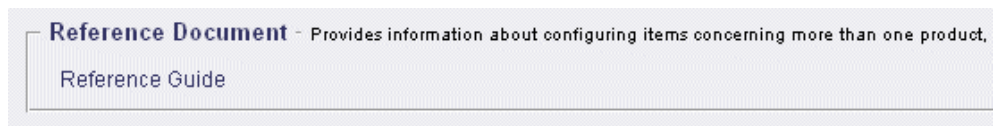


This section allows you to view user documentation on individual Webwasher products.

To view any of the documents listed here, click on the [PDF](#) link in the same line. This will open a [.pdf](#) format version of the document.

Reference Document

The [Reference Document](#) section looks like this:



This section allows you to view the Webwasher Reference Guide.

To view it, click on the [PDF](#) link in the same line. This will open a [.pdf](#) format version of the document.

2.5.2 Documentation on Special Products

The *Documentation on Special Products* tab looks like this:

The screenshot shows a web interface with three tabs: 'Documentation on Main Products', 'Documentation on Special Products' (selected), and 'Additional Documentation'. The 'Documentation on Special Products' tab contains four sections, each with a title, a brief description, and a list of documents with PDF links.

Section	Description	Documents
Content Reporter Documents	Provide information about installing, configuring and operating the Webwasher reporting tool	<ul style="list-style-type: none"> Content Reporter Installation and Configuration Guide (→ PDF) Content Reporter User's Guide for Reporting (→ PDF)
Instant Message Filter Documents	Provide information about installing, configuring and operating the Webwasher Instant Messenger	<ul style="list-style-type: none"> Instant Message Filter Installation Guide (→ PDF) Instant Message Filter User's Guide (→ PDF)
Special Environment Documents	Provide information about setting up Webwasher or products running with it in a special environment	<ul style="list-style-type: none"> Setting Up NetCache with ICAP (→ PDF) Setting Up Webwasher® on Microsoft ISA Server (→ PDF) Setting Up Webwasher® with Blue Coat™ (→ PDF) NTML Agent Set-up Guide (→ PDF) HSM Agent Set-up Guide (→ PDF)
Appliance Documents	Provide information about the Webwasher appliances	<ul style="list-style-type: none"> Appliance Installation and Configuration Guide (→ PDF) Appliance Upgrade Guide (→ PDF)

There are four sections on this tab:

- [Content Reporter Documents](#)
- [Instant Message Filter Documents](#)
- [Special Environment Documents](#)
- [Appliance Documents](#)

They are described in the following.

Content Reporter Documents

The *Content Reporter Documents* section looks like this:

The screenshot shows a section titled 'Content Reporter Documents' with a description: 'Provide information about installing, configuring and operating the Webwasher reporting tool'. Below the description are two document titles:

- Content Reporter Installation and Configuration Guide
- Content Reporter User's Guide for Reporting

This section allows you to view user documentation on the Webwasher reporting tool.

To view any of the documents listed here, click on the [PDF](#) link in the same line. This will open a [.pdf](#) format version of the document.

Instant Message Filter Documents

The *Instant Message Filter Documents* section looks like this:

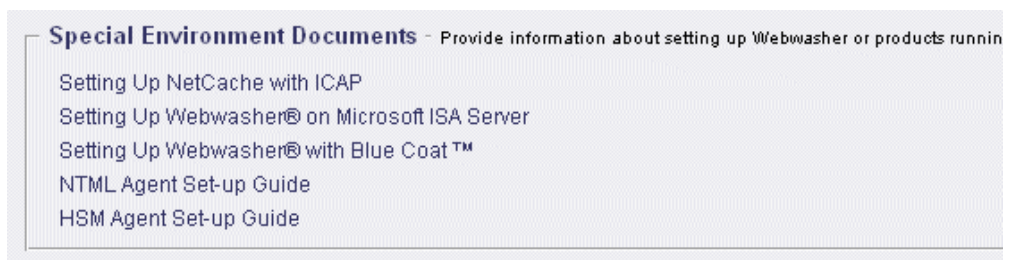


This section allows you to view user documentation on the Webwasher instant message filtering tool.

To view any of the documents listed here, click on the *PDF* link in the same line. This will open a *.pdf* format version of the document.

Special Environment Documents

The *Special Environment Documents* section looks like this:



This section allows you to view user documentation on setting up Webwasher or products running with it in a special environment..

To view any of the documents listed here, click on the *PDF* link in the same line. This will open a *.pdf* format version of the document.

Appliance Documents

The *Appliance Documents* section looks like this:

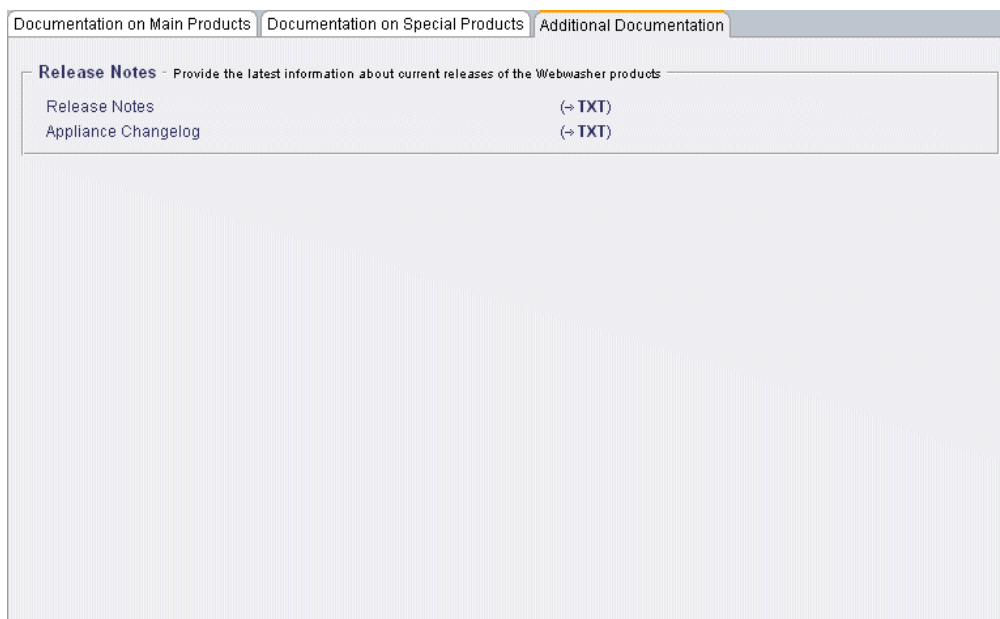


This section allows you to view user documentation on the Webwasher appliance.

To view any of the documents listed here, click on the [PDF](#) link in the same line. This will open a [.pdf](#) format version of the document.

2.5.3 Additional Documentation

The [Additional Documentation](#) tab looks like this:



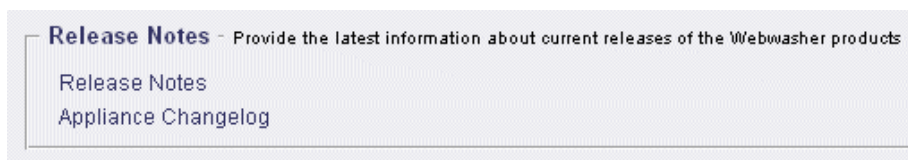
There is one section on this tab:

- [Release Notes](#)

It is described in the following.

Release Notes

The [Release Notes](#) section looks like this:



This section allows you to view release notes and other documents containing the latest information on the Webwasher products.

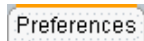
To view any of the documents listed here, click on the [TXT](#) link in the same line. This will open a [.txt](#) format version of the document.

2.6 Preferences

The *Preferences* options are invoked by clicking on the corresponding button under *Home*:



The options are arranged under the following tab:

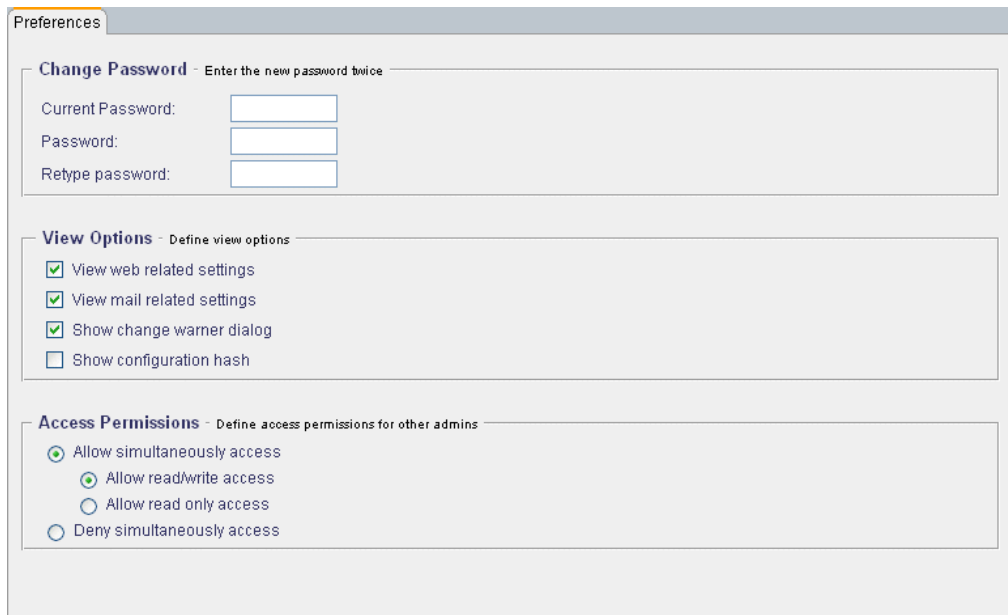


They are described in the upcoming section:

- *Preferences*, see [2.6.1](#)

2.6.1 Preferences

The *Preferences* tab looks like this:



The screenshot shows the 'Preferences' tab with the following sections:

- Change Password** - Enter the new password twice
 - Current Password:
 - Password:
 - Retype password:
- View Options** - Define view options
 - View web related settings
 - View mail related settings
 - Show change warning dialog
 - Show configuration hash
- Access Permissions** - Define access permissions for other admins
 - Allow simultaneously access
 - Allow read/write access
 - Allow read only access
 - Deny simultaneously access

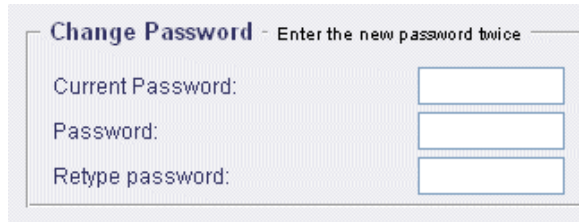
There are three sections on this tab:

- *Change Password*
- *View Options*
- *Access Permissions*

They are described in the following.

Change Password

The *Change Password* section looks like this:



The screenshot shows a form titled "Change Password" with the subtitle "Enter the new password twice". It contains three input fields: "Current Password:", "Password:", and "Retype password:", each with a corresponding text box.

Using this section, you can change the password you are using for access to Webwasher.

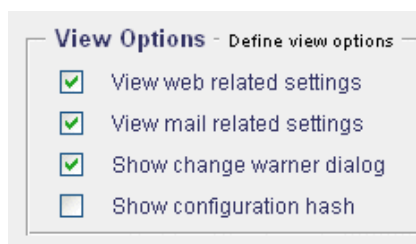
After specifying the appropriate input here, click on *Apply Changes* to make the new password effective.

Use the following input fields to change your password:

- *Current Password*
Enter your current Webwasher password here.
- *Password*
Enter the new password here.
- *Retype password*
Enter the new password here a second time to confirm it.

View Options

The *View Options* section looks like this:



The screenshot shows a form titled "View Options" with the subtitle "Define view options". It contains four checkboxes with labels: "View web related settings", "View mail related settings", "Show change warner dialog", and "Show configuration hash". The first three checkboxes are checked, and the last one is unchecked.

Using this section, you can configure what you would like the Web interface to display or not.

If you are only interested in viewing and configuring settings for Web traffic, you can hide the e-mail related settings and vice versa.

Furthermore, you can configure the change warner dialog and the configuration hash to be displayed or not.

After specifying the appropriate settings, click on *Apply Changes* to make them effective.

Use the following checkboxes to configure view options:

- *View web related settings*

Make sure this checkbox is marked if you want to view the Web related settings.

- *View web mail related settings*

Make sure this checkbox is marked if you want to view the e-mail related settings.

- *Show change warner*

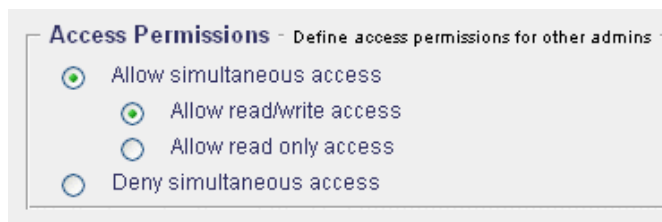
Make sure this checkbox is marked if you want the change warner dialog to appear whenever you are attempting to leave a tab without saving changed settings.

- *Show change warner*

Mark this checkbox to have the configuration hash displayed at the top of the Web interface area.

Access Permissions

The *Access Permissions* section looks like this:



Using this section, you can configure permissions to control access to Web-washer. While you are logged in as administrator, other administrators, i. e. other users in administrator roles, might also try to log in.

You can allow their simultaneous access, restrict it to read-only or even deny it completely.

To what extent you are allowed to configure access permissions for other administrators, depends on your seniority level. This is measured by a value between 0 and 100. You can only configure permissions for administrators with seniority levels lower than your own.

On the other hand, you may find your right to access Webwasher restricted or denied when trying to log in because an administrator with an equal or higher seniority level is currently logged in and has configured the corresponding settings.

So, if your seniority level is e. g. 80 and you have configured read-only access for other administrators while you are logged in, this will apply to all administrators with a seniority level of 80 or below.

If an administrator with a level of e. g. 60 logs in, a window will open providing access in read-only mode. At the same time, the number of sessions is displayed that are currently active, as well as the number of sessions where the seniority level is equal to or higher than that of the administrator who is trying to log in.

Furthermore, the number of sessions is displayed where this administrator is allowed to modify access permissions. In this case, there are no such sessions because someone with an equal or higher seniority level, i. e. you, has already configured the corresponding settings in a particular way.

This administrator now has the choice of logging in with read-only access or not.

On the other hand, if an administrator with a seniority level of e. g. 100 logs in, this administrator is entitled to modify what you configured since your seniority level is only 80. This modification will also apply to sessions where other administrators are already logged in.

The seniority level is configured on the *Role Definition* tab under *User Management > Administrators*. Click on the *Edit Role Permissions* button there to open a window, where you can configure a value for the seniority level.

After specifying the appropriate settings here, click on *Apply Changes* to make them effective.

Use the following radio buttons to configure access permissions:

- *Allow simultaneous access*

Make sure this radio button is checked if you want to allow simultaneous access. Furthermore, specify what kind of simultaneous access should be allowed:

- *Allow read/write access*

Make sure this radio button is checked if you want to allow read/write access.

— *Allow read only access*

Check this radio button to allow read only access.

- *Deny simultaneous access*

Check this radio button to deny simultaneous access.

2.7 License

The *License* options are invoked by clicking on the corresponding button under *Home*:

The options are arranged under the following tabs:

They are described in the upcoming sections:

- *Information*, see [2.7.1](#)
- *Notification*, see [2.7.2](#)

2.7.1 Information

The *Information* tab looks like this:

The screenshot shows a web interface with two tabs: 'Information' (selected) and 'Notification'. The 'Information' section is divided into four main areas:

- License Information:** A table showing details about the license.

Company Name	Webwasher 60 Test
Number of Clients	25000
Current Clients	0
Time Limit	01.07.2006 - 31.06.2008
Evaluation License	Yes
Customer number	1061
Key number / System number	1 / 1
- Webwasher End User License Agreement:** A text block stating that the installation and deployment of Webwasher software products are exclusively governed by the terms as set forth in webwasher AG's Standard Terms and Conditions. It provides a link to the most recent version: http://www.webwasher.com/enterprise/downloadinformationterms_and_conditions.pdf.
- Import License:** A section with a search input field, a 'Durchsuchen...' button, and a message 'You have to accept the EULA first'. Below it is a checkbox labeled 'I have read the → end user license agreement and accept it'.
- Licensed Products:** A list of products, each with an icon, a name, and a status.

	URL Filter	Included
	Anti Malware	Included
	Anti Virus	Included
	Anti Spam	Included
	Content Protection	Included
	SSL Scanner	Included
	Content Reporter	Included
	Instant Message Filter	Included

There are four sections on this tab:

- *License Information*
- *Webwasher End User License Agreement*
- *Import License*
- *Licensed Products*

They are described in the following.

License Information

The *License Information* section looks like this:

License Information	
Company Name	Webwasher 60 Test
Number of Clients	25000
Current Clients	0
Time Limit	01.07.2006 - 31.06.2008
Evaluation License	Yes
Customer number	1061
Key number / System number	1 / 1

This section displays information regarding the license of the Webwasher software.

Information is provided on the company that purchased the license, the time interval during which the license is valid and other licensing issues.

Webwasher End User License Agreement

The *Webwasher End User License Agreement* section looks like this:

Webwasher End User License Agreement

The installation and deployment of Webwasher software products are exclusively governed by the the most recent version at

-> http://www.webwasher.com/enterprise/download/information/terms_and_conditions.pdf.

This section allows you to view the most recent version of the Webwasher end user license agreement.

To view the agreement, click on the link that is provided here.

Import License

The *Import License* section looks like this:

Import License

You have to accept the EULA

I have read the -> **end user license agreement** and accept it

Using this section, you can import a license for the Webwasher software.

To import a license, proceed as follows:

1. Click on the [Browse](#) button provided here and browse for the license file you want to import.

[Browse](#)

Before you can import it, you will have to accept the end user license agreement. To read it, click on the [end user license agreement](#) link provided here.

2. If you accept the agreement, mark the checkbox labeled [I have read ...](#)

I have read the → [end user license agreement](#) and accept it

This will turn the button saying [You have to accept the EULA first](#) into one saying [Activate License](#).

3. Click on this button to import the license.

[Activate License](#)

Licensed Products

The [Licensed Products](#) section looks like this:

Licensed Products		
	URL Filter	Included
	Anti Malware	Included
	Anti Virus	Included
	Anti Spam	Included
	Content Protection	Included
	SSL Scanner	Included
	Content Reporter	Included
	Instant Message Filter	Included

This section displays the Webwasher products and provides information as to whether they are covered by your license.

For an overview of these products, see 1.5.

2.7.2 Notification

The *Notification* tab looks like this:

Information | **Notification**

System Notifications - Send notifications upon license status ?

Send notification upon license expiry
Recipient:

Send notification if number of licensed clients will soon be exceeded
The Recipient from 'Send notification upon license expiry' will be used

Before sending system notifications you must configure the delivery options [Edit Notification Mail Server](#)

Test Notification Settings: [Send Test Messages](#)

Too Many Clients - Writes system log messages if connections were refused due to heavy work load or license exhaustion ?

Enable message to be written to system log
Message text:

There are two sections on this tab:

- *System Notifications*
- *Too Many Clients*

They are described in the following.

System Notifications

The *System Notifications* section looks like this:

System Notifications - Send notifications upon license status

Send notification upon license expiry
Recipient:

Send notification if number of licensed clients will soon be exceeded
The Recipient from 'Send notification upon license expiry' will be used

Before sending system notifications you must configure the delivery options [Edit Notification Mail](#)

Test Notification Settings: [Send Test Messages](#)

Using this section, you can configure e-mail notifications on license issues. These will be sent to the e-mail address of the recipient you specify here.

After specifying the appropriate information, click on [Apply Changes](#) to make your settings effective.

Use the following items to configure the system notifications:

- [Send notification upon license expiry](#)

Make sure the checkbox provided here is marked if you want to use this option, and enter the recipient of the notification in the [Recipient](#) input field.

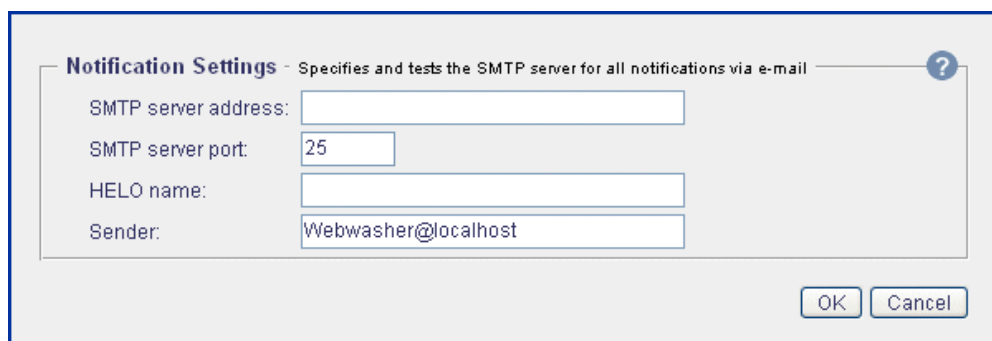
- [Send notification if number of licensed clients will soon be exceeded](#)

Make sure the checkbox provided here is marked if you want to use this option.

The recipient of this notification will be the one entered in the [Recipient](#) input field above.

To configure the settings for the server used to process the notifications, click on the button labeled [Edit Notification Mail Server](#).

This will open a window where you can specify the appropriate settings:



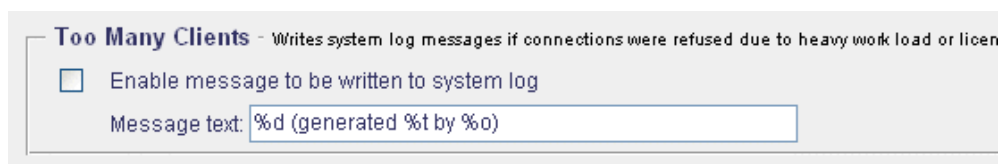
The screenshot shows a dialog box titled "Notification Settings" with a subtitle "Specifies and tests the SMTP server for all notifications via e-mail". The dialog contains four input fields: "SMTP server address:" (empty), "SMTP server port:" (containing "25"), "HELO name:" (empty), and "Sender:" (containing "Webwasher@localhost"). There are "OK" and "Cancel" buttons at the bottom right. A help icon (?) is in the top right corner.

After specifying the settings, click [OK](#) to make them effective.

Furthermore, there is a button labeled [Send Test Messages](#) in this section. Click on this button to test your settings.

Too Many Clients

The [Too Many Clients](#) section looks like this:



The screenshot shows a dialog box titled "Too Many Clients" with a subtitle "Writes system log messages if connections were refused due to heavy work load or licen". It contains a checkbox labeled "Enable message to be written to system log" which is currently unchecked. Below the checkbox is a text input field labeled "Message text:" containing the text "%d (generated %t by %o)".

Using this section, you can configure messages to be written to the system log if connections were refused due to heavy work load or license exhaustion.

After specifying the appropriate settings, click on [Apply Changes](#) to make them effective.

Use the following items to configure log messages:

- [Enable message to be written to system log](#)

Mark this checkbox if you want log messages to be written to the system log.

— [Message text](#)

In this input field, enter the message text. The default text is:

%d (generated %t by %o)

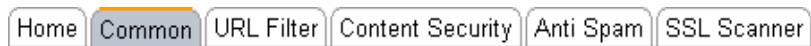
You can use the variable log file parameters appearing in the default text to set up your own message text. Furthermore, you can use an event name and a severity parameter.

The following table lists these parameters and their meanings:

<i>%e</i>	Short name of the event that caused the log file message to be written
<i>%d</i>	Description of the event
<i>%s</i>	Severity of the event
<i>% t</i>	Local time and timezone of the host that generated the log file message
<i>%o</i>	FQDN name of the host

Common

The features that are described in this chapter are accessible over the *Common* tab of the Web interface:



These are filtering features that are common to the SSL Scanner and other Webwasher products, e. g. media type filters, the document inspector, the white list, etc.

The upcoming sections describe how to handle these features. The description begins with an overview.

3.1 Overview

The following overview shows the sections that are in this chapter:

User's Guide SSL Scanner	
<i>Introduction</i>	
<i>Home</i>	
Common	Overview – <i>this section</i>
<i>Policy Settings</i>	Media Type Filters, see 3.2 Document Inspector, see 3.3 Archive Handler, see 3.4 Generic Header Filter, see 3.5 Generic Body Filter, see 3.6 Advertising Filters, see 3.7 Privacy Filters, see 3.8 Text Categorization, see 3.9 White List, see 3.10
<i>Policy-Independent Settings</i>	User-Defined Categories, see 3.11 Media Type Catalog, see 3.12
<i>SSL Scanner</i>	

3.2 Media Type Filters

The *Media Type Filters* options are invoked by clicking on the corresponding button under *Common*:



If you want to enable any of these options, mark the checkbox that is on this button.

Then click on *Apply Changes* to make this setting effective.

These are policy-dependent options, i. e. they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled *Policy*, which is located above the *Media Type Filters* button:

Policy:
 default ▼
 Media Type Filters □

The options are arranged under the following tabs:

Actions | Media Type Black List | Media Type White List

They are described in the upcoming sections:

- *Actions*, see [3.2.1](#)
- *Media Type Black List*, see [3.2.2](#)
- *Media Type White List*, see [3.2.3](#)

3.2.1 Actions

The *Actions* tab looks like this:

Actions | Media Type Black List | Media Type White List

Media Type Filter - Manages the flow of media types for mail and Web downloads

Default action for unlisted media types	WEB	Block	MAIL	Allow
Entry found in Media Type Black List	WEB	Block	MAIL	Replace and Quarantine
Entry found in Media Type White List	WEB	Allow	MAIL	Allow
Non-rectifiable media types with magic bytes mismatch	WEB	Block	MAIL	Replace and Quarantine
Response without Content-Type header	WEB	Allow	MAIL	Allow

Web Upload Filter - Controls the flow of outbound user-originating files via HTTP and FTP

Maximal size of uploaded parameter kb

Forbid uploads of all files (HTTP)

Forbid uploads of all files (FTP)

Default action for unlisted media types	WEB	Allow
Entry found in Media Type Black List	WEB	Block
Entry found in Media Type White List	WEB	Allow
Content not validated by magic bytes	WEB	Allow

Go to → **REOMOD Settings** to enable 'Apply configured filters on uploaded and posted data' to use the Web Upload Filter

There are two sections on this tab:

- *Media Type Filter*
- *Web Upload Filter*

They are described in the following.

Media Type Filter

The *Media Type Filter* section looks like this:

Configuration Item	WEB	MAIL
Default action for unlisted media types	Block	
Entry found in Media Type Black List	Block	
Entry found in Media Type White List	Allow	
Non-rectifiable media types with magic bytes mismatch	Block	
Response without Content-Type header	Allow	

Using this section, you can configure actions, e. g. *Block*, *Block*, *log and notify*, *Allow*, etc., for the Media Type Filter.

This filter manages the flow of incoming media types for HTTP and FTP downloads, as well as for SMTP.

A media (content) type is a general category of data content, such as an application, audio content, a text message, an image, a video stream, etc. The media type tells the application that receives the data what kind of application is needed to process the content, e. g. Real Audio is to play the audio content for a user. Each of these media types also have subtypes, e. g. the text media type has four subtypes: plain, rich text, enriched, and tab-separated values.

The actions that you configure here will be executed according to the result achieved by the Media Type Filter for a filtered object.

You can also configure different actions for Web and e-mail traffic.

After specifying the appropriate settings here, click on *Apply Changes* to make them effective.

Use the drop-down lists provided here to configure actions in the following way:

- *Default action for unlisted media types*

Should this filter find a media type that is not currently listed in the Media Type White List or Black List, this is what will happen to it.

- *Entry found in Media Type Black List*

The actions configured here will be executed for media types that are found in the Media Type Black List.

- *Entry found in Media Type White List*

The actions configured here will be executed for media types that are found in the Media Type White List.

- *Non-rectifiable media types with magic bytes mismatch*

The actions configured here will be executed when content types do not match their magic byte sequence.

So, e. g., a *JPEG* image named as a *GIF* file would be affected by a filtering action, even though each of these media types are acceptable.

- *Response without Content-Type header*

The actions configured here will be executed when media type information is contained in a response header..

Web Upload Filter

The *Web Upload Filter* section looks like this:

Using this section, you can configure actions, e. g. *Block*, *Block*, *log and notify*, *Allow*, etc., for the Web Upload Filter.

This filter protects corporate privacy and sensitive data by filtering what employees send out, e. g. FTP uploads or file attachments sent through common HTTP-based Web mail services, such as Hotmail or GMX.

You can limit the size that uploads may have or even forbid uploads of all HTTP and FTP files.

The actions that you configure here will be executed according to the result achieved by the Media Type Filter for a filtered object.

You can also configure different actions for Web and e-mail traffic.

After specifying the appropriate settings here, click on *Apply Changes* to make them effective.

Furthermore, you need to enable an option on the *REQMOD Settings* tab to use this filter. To do this, click on the *REQMOD Settings* link provided at the bottom of this section. The option in question is labeled *Apply configured filters on uploaded and posted data*.

Use the drop-down lists provided here to configure actions for the Web Upload Filter:

- *Maximal size of uploaded parameter . . . kb*

In the input field provided here, enter a value to limit the size limit (in KB) of uploads.

- *Forbid uploads of all files (HTTP)*

Mark this checkbox, to forbid uploads of all HTTP files.

- *Forbid uploads of all files (FTP)*

Mark this checkbox, to forbid uploads of all FTP files.

- *Default action for unlisted media types*

Should this filter find a media type that is not currently listed in the Media Type White List or Black List, this is what will happen to it.

- *Entry found in Media Type Black List*

The actions configured here will be executed for media types that are found in the Media Type Black List.

- *Entry found in Media Type White List*

The actions configured here will be executed for media types that are found in the Media Type White List.

- *Content not validated by magic bytes*

The actions configured here will be executed when content types do not match their magic byte sequence.

So, e. g., a *JPEG* image named as a *GIF* file would be affected by a filtering action, even though each of these media types are acceptable.

3.2.2 Media Type Black List

The *Media Type Black List* tab looks like this:

The screenshot shows a web interface for configuring a Media Type Black List. At the top, there are three tabs: 'Actions', 'Media Type Black List' (which is selected), and 'Media Type White List'. Below the tabs, the main content area is titled 'Media Type Black List - Defines media types that will be blocked'. It features a form with a dropdown menu for 'Select media type from catalog' (currently showing 'application/ace'), a text input for 'Description' (placeholder: '<Enter description here>'), and two checkboxes: 'Ignore in Media Type Filter' and 'Ignore in Web Upload Filter'. Below the form are two buttons: 'Add to Media Type Black List' and 'Add to all policies'. A summary line indicates 'Found 1 entries with *, *' and 'Number of entries per page: 10'. Below this is a table with columns 'Select', 'Media Type', and 'Description'. The table contains one entry for 'application/ace' with the description '<Enter description here>'. To the right of the table are checkboxes for 'Ignore in media type filter' and 'Ignore in web upload filter'. At the bottom of the table area are 'Select All' and 'Delete Selected' buttons.

Select	Media Type	Description
<input type="checkbox"/>	application/ace	<Enter description here>

There is one section on this tab:

- *Media Type Black List*

It is described in the following.

Media Type Black List

The *Media Type Black List* section looks like this:

Media Type Black List - Defines media types that will be blocked

Select media type from catalog: application/ace

Description: <Enter description here>

Ignore in Media Type Filter Ignore in Web Upload Filter

Add to all policies

Found 1 entries with *, *

Select	Media Type	Description
<input type="checkbox"/>	application/ace	<Enter description here>

Select All

Using this section, you can add a media type to the Media Type Black List. Objects belonging to the media types on this list will be blocked.

To add a media type to the black list, use the area labeled:

- *Service Name*

In this input field, enter the service name.

Select the media type you want to have blacklisted from the drop-down list provided here, e. g. *application/ace*.

Furthermore, use the following items when adding a media type:

— *Description*

Input in this field is optional. You may enter a description of the media type here.

— *Ignore in Media Type Filter*

If this option is enabled, the media type in question will be ignored when the Media Type Filter is applied to Web and e-mail downloads.

— *Ignore in Web Upload Filter*

If this option is enabled, the media type in question will be ignored when the Web Upload Filter is applied to outbound user-originating files via HTTP, HTTPS and FTP.

— *Add to Media Type Black List*

After selecting a media type, click on this button to add it to the list.

This addition will be valid only under the policy you are currently configuring.

To add a media type to the black list for all policies, mark the checkbox labeled *Add to all policies* before clicking on the button.

The Media Type Black List is displayed at the bottom of this section.

To display only a particular number of list entries at a time, type this number in the input field labeled *Number of entries per page* and enter it using the *Enter* key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To sort the list in ascending or descending order, click on the symbol next to the *Media Type* or *Description* column heading.

To edit an entry, type the appropriate text in the input field of the *Description* column and enable or disable the *Ignore in media type filter* and *Ignore in media type filter* options.

Then click on *Apply Changes* to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- *Filter*

Type a filter expression in the input field of the *Media Type* or *Description* column or in both and enter this using the *Enter* key of your keyboard. The list will then display only entries matching the filter.

- *Delete Selected*

Select the entry you wish to delete by marking the *Select* checkbox next to it and click on this button. You can delete more than one entry in one go.

To delete all entries, mark the *Select all* checkbox and click on this button.

3.2.3 Media Type White List

The *Media Type White List* tab looks like this:

The screenshot shows a web interface with three tabs: 'Actions', 'Media Type Black List', and 'Media Type White List'. The 'Media Type White List' tab is active. The main heading is 'Media Type White List - Defines media types that will be allowed'. Below this, there is a form to add a new media type. It includes a dropdown menu for 'Select media type from catalog' with 'application/ace' selected, a text input for 'Description' with the placeholder '<Enter description here>', and two checkboxes: 'Ignore in Media Type Filter' and 'Ignore in Web Upload Filter'. At the bottom of the form are two buttons: 'Add to Media Type White List' and 'Add to all policies'. Below the form, it says 'Found 1 entries with *'. To the right, there is a 'Number of entries per page:' dropdown set to '10'. A table with columns 'Select', 'Media Type', and 'Description' is shown. The table has one row with a checkbox, 'message/rfc822', and a description input field. To the right of the row are two checkboxes: 'Ignore in media type filter' and 'Ignore in web upload filter'. At the bottom of the table are 'Select All' and 'Delete Selected' buttons.

There is one section on this tab:

- *Media Type White List*

It is described in the following.

Media Type White List

The *Media Type White List* section looks like this:

Media Type White List - Defines media types that will be allowed

Select media type from catalog:

Description:

Ignore in Media Type Filter Ignore in Web Upload Filter

Add to all policies

Found 1 entries with **

Select	Media Type	Description
<input type="checkbox"/>	message/rfc822	

Select All

Using this section, you can add a media type to the Media Type White List. Objects belonging to the media types on this list will be allowed.

To add a media type to the white list, use the area labeled:

- *Select media type from catalog*

Select the media type you want to include in the white list from the drop-down list provided here, e. g. *application/ace*.

Furthermore, use the following items when adding a media type:

— *Description*

Input in this field is optional. You may enter a description of the media type here.

— *Ignore in Media Type Filter*

If this option is enabled, the media type in question will be ignored when the Media Type Filter is applied to Web and e-mail downloads.

— *Ignore in Web Upload Filter*

If this option is enabled, the media type in question will be ignored when the Web Upload Filter is applied to outbound user-originating files via HTTP, HTTPS and FTP.

— *Add to Media Type White List*

After selecting a media type, click on this button to add it to the list.

This addition will be valid only under the policy you are currently configuring.

To add a media type to the white list for all policies, mark the checkbox labeled *Add to all policies* before clicking on the button.

The Media Type White List is displayed at the bottom of this section.

To display only a particular number of list entries at a time, type this number in the input field labeled *Number of entries per page* and enter it using the *Enter* key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To sort the list in ascending or descending order, click on the symbol next to the *Media Type* or *Description* column heading.

To edit an entry, type the appropriate text in the input field of the *Description* column and enable or disable the *Ignore in media type filter* and *Ignore in media type filter* options.

Then click on *Apply Changes* to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- *Filter*

Type a filter expression in the input field of the *Media Type* or *Description* column or in both and enter this using the *Enter* key of your keyboard. The list will then display only entries matching the filter.

- *Delete Selected*

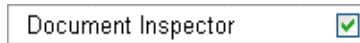
Select the entry you wish to delete by marking the *Select* checkbox next to it and click on this button. You can delete more than one entry in one go.

To delete all entries, mark the *Select all* checkbox and click on this button.

3.3

Document Inspector

The *Document Inspector* options are invoked by clicking on the corresponding button under *Common*:

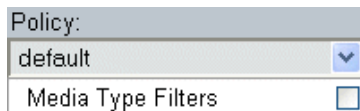


If you want to enable any of these options, make sure the checkbox on this button is also marked. The checkbox is marked by default.

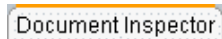
After modifying the setting of this checkbox, click on *Apply Changes* to make the modification effective.

These are policy-dependent options, i. e. they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled *Policy*, which is located above the *Media Type Filters* button:



The options are arranged under the following tab:

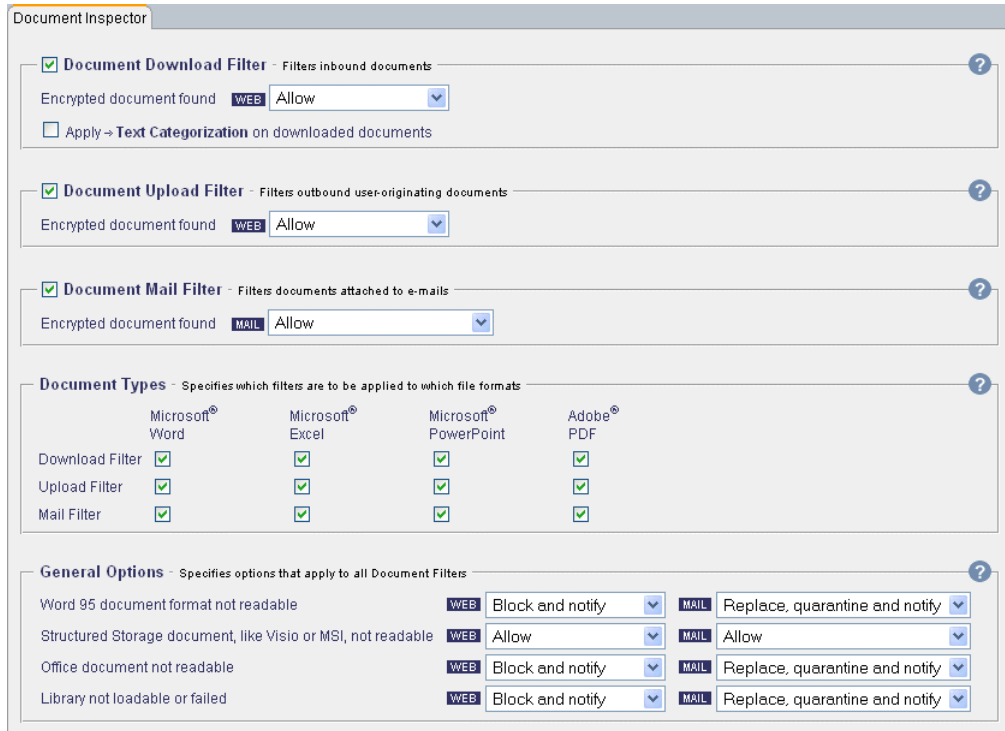


They are described in the upcoming section:

- *Document Inspector*, see [3.3.1](#)

3.3.1 Document Inspector

The *Document Inspector* tab looks like this:



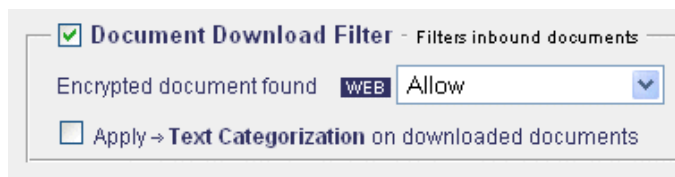
There are five sections on this tab:

- *Document Download Filter*
- *Document Upload Filter*
- *Document Mail Filter*
- *Document Types*
- *General Options*

They are described in the following.

Document Download Filter

The *Document Download Filter* section looks like this:



Using this section, you can configure actions for inbound office documents that may enter your corporate network from the Web and are potentially malicious.

The document formats that can be filtered include Microsoft Word 97-2003, Microsoft Excel 95-2003, Microsoft PowerPoint 95-2003 and all known versions of Adobe Portable Document Format (PDF).

These documents may contain “active” content. Microsoft Word, Excel and PowerPoint support ActiveX controls and macros, while PDF supports embedded JavaScript.

This active content may be hostile rather than friendly, so for full protection against files that are embedded into Microsoft Office or PDF documents, you should use the filter provided by the Document Inspector to inspect these documents and block malicious content from entering your corporate network.

In addition to this filter, you can apply text categorization to these documents.

If you want to use this filter, make sure the checkbox next to the section heading is marked. The checkbox is marked by default.

After specifying the appropriate settings, click on *Apply Changes* to make them effective.

Use the following items to configure actions for office documents:

- *Encrypted document found*

From the drop-down list provided here, select an action, e. g. *Block* or *Allow*. This action will be taken if the filter detects an inbound office document that is potentially malicious.

- *Apply Text Categorization*

Mark the checkbox provided here, to apply text categorization actions to inbound office documents.

To view or modify the actions that are currently configured for these actions, click on the *Text Categorization* link in the checkbox inscription.

This will take you to the *Text Categorization* tab, where you have access to the corresponding settings.

Document Upload Filter

The *Document Upload Filter* section looks like this:



Using this section, you can configure actions for outbound user-originating office documents that are potentially malicious.

The document formats that can be filtered include Microsoft Word 97-2003, Microsoft Excel 95-2003, Microsoft PowerPoint 95-2003 and all known versions of Adobe Portable Document Format (PDF).

If you want to use this filter, make sure the checkbox next to the section heading is marked. The checkbox is marked by default.

After specifying the appropriate settings, click on *Apply Changes* to make them effective.

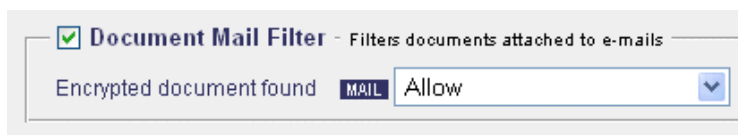
Use the following drop-down list to configure actions for office documents:

- *Encrypted document found*

Select an action here, e. g. *Block* or *Allow*. This action will be taken if the filter detects an inbound office document that is potentially malicious.

Document Mail Filter

The *Document Mail Filter* section looks like this:



Using this section, you can configure actions for office documents that are attached to e-mails, e. g. a *.pdf* format document.

The document formats that can be filtered include Microsoft Word 97-2003, Microsoft Excel 95-2003, Microsoft PowerPoint 95-2003 and all known versions of Adobe Portable Document Format (PDF).

These documents may contain “active” content. Microsoft Word, Excel and PowerPoint support ActiveX controls and macros, while PDF supports embedded JavaScript.

This active content may be hostile rather than friendly, so for full protection against files that are embedded into Microsoft Office or PDF documents, you should use the filter provided by the Document Inspector to inspect these documents and block malicious content from entering your corporate network.

If you want to use this filter, make sure the checkbox next to the section heading is marked. The checkbox is marked by default.

After specifying the appropriate settings, click on *Apply Changes* to make them effective.

Use the following items to configure actions for office documents:

- *Encrypted document found*

From the drop-down list provided here, select an action, e. g. *Drop, Drop and Quarantine* or *Allow*.

This action will be taken if the filter detects an office document attached to an e-mail that is potentially malicious.

Document Types

The *Document Types* section looks like this:

Document Types - Specifies which filters are to be applied to which file formats			
	Microsoft® Word	Microsoft® Excel	Microsoft® PowerPoint
Download Filter	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Upload Filter	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Mail Filter	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Using this section, you can configure which of the filters that are accessible over the other sections of this tab should be applied to which document formats.

The document formats that can be filtered include Microsoft Word 97-2003, Microsoft Excel 95-2003, Microsoft PowerPoint 95-2003 and all known versions of Adobe Portable Document Format (PDF).

By default, all filters are configured to apply to all formats.

After modifying these settings, click on *Apply Changes* to make the modification effective.

Use the following checkboxes to modify the assignment of filters to document formats:

- *Download Filter*

Mark or clear the checkboxes in this line to have the download filter apply to the corresponding document formats.

- *Upload Filter*

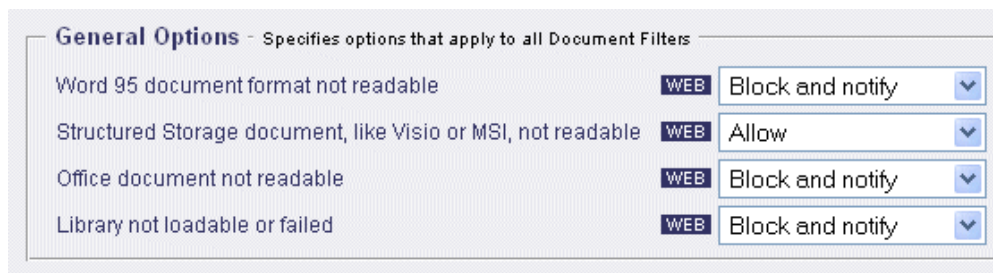
Mark or clear the checkboxes in this line to have the upload filter apply to the corresponding document formats.

- *Mail Filter*

Mark or clear the checkboxes in this line to have the mail filter apply to the corresponding document formats.

General Options

The *General Options* section looks like this:



Using this section, you can configure filtering conditions and actions for office documents that will apply to all the filters made accessible over the other sections of this tab.

You can configure different actions for documents in Web and e-mail traffic.

After specifying the appropriate settings, click on *Apply Changes* to make them effective.

Use the following items to configure filtering conditions and actions:

- *Word 95 document format not readable*

From the drop-down lists provided here, select actions for documents in Web and e-mail traffic, e. g. *Block* or *Allow*.

These are required because this format is not supported by the Document Inspector, which means the documents in question are unreadable for this filter.

- *Structured Storage document, like Visio or MSI, not readable*

From the drop-down lists provided here, select actions for documents in Web and e-mail traffic, e. g. *Block* or *Allow*.

These actions will be executed if a structured storage document is unreadable.

- *Office document not readable*

From the drop-down lists provided here, select actions for documents in Web and e-mail traffic, e. g. *Block* or *Allow*.

These actions will be executed for any type of office documents that are unreadable, perhaps due to encryption.

- *Library not loadable or failed*

From the drop-down lists provided here, select actions for documents in Web and e-mail traffic, e. g. *Block* or *Allow*.

These actions will be executed if the Document Inspector library could not be loaded.

3.4

Archive Handler

The *Archive Handler* options are invoked by clicking on the corresponding button under *Common*:

 Archive Handler

If you want to enable any of these options, make sure the checkbox on this button is also marked. The checkbox is marked by default.

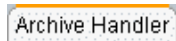
After modifying the setting of this checkbox, click on *Apply Changes* to make the modification effective.

These are policy-dependent options, i. e. they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled *Policy*, which is located above the *Media Type Filters* button:



The options are arranged under the following tab:

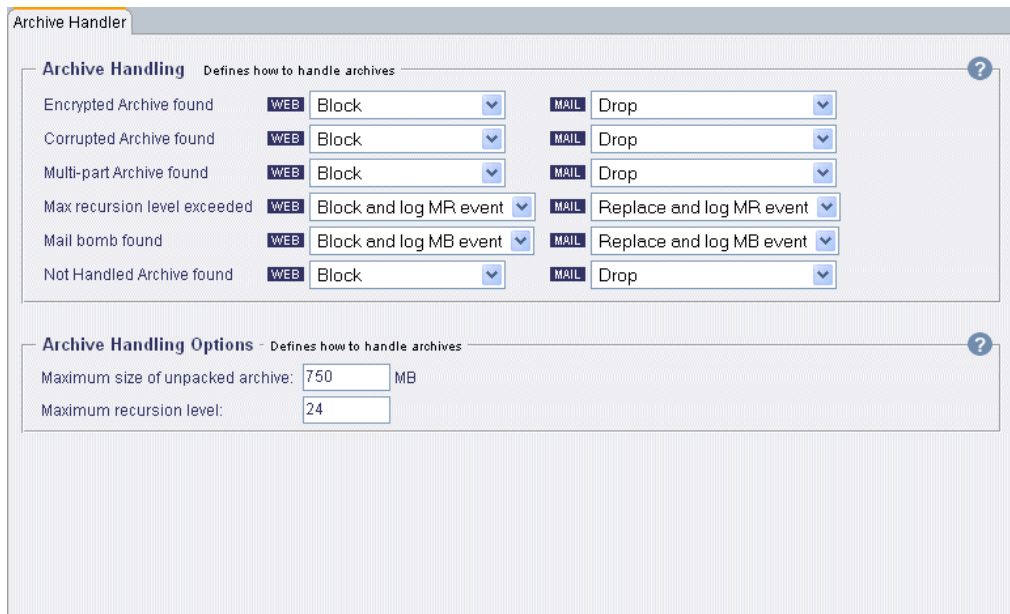


They are described in the upcoming section:

- *Archive Handler*, see [3.4.1](#)

3.4.1 Archive Handler

The *Archive Handler* tab looks like this:



There are two sections on this tab:

- *Archive Handling*
- *Archive Handling Options*

They are described in the following.

Archive Handling

The *Archive Handling* section looks like this:

Event	WEB Action	MAIL Action
Encrypted Archive found	Block	Drop
Corrupted Archive found	Block	Drop
Multi-part Archive found	Block	Drop
Max recursion level exceeded	Block and log MR event	Replace and log
Mail bomb found	Block and log MB event	Replace and log
Not Handled Archive found	Block	Drop

Using this section, you can configure blocking and other actions for encrypted, corrupted, multi-part archives, archives containing mail bombs (an archive is a mail bomb if its content size exceeds the limit set by the user), and archives exceeding the maximum recursion level, i. e. how deep archives are nested within each other.

The size and recursion level limits are configured in the *Archive Handling Options* section, which is also provided on this tab.

If a virus is contained within an archive that is compressed, the virus cannot be detected and prevented from downloading.

The Archive Handler decompresses the members of an archive one-by-one, and passes them on to the virus scanner. When the archive member containing the virus is decompressed, virus scanner detects the virus, so the archive can be blocked.

You can configure different actions for archives in Web and e-mail traffic.

After selecting these actions from the drop-down lists provided here, click on *Apply Changes* to make your settings effective.

Archive Handling Options

The *Archive Handling Options* section looks like this:

Option	Value	Unit
Maximum size of unpacked archive:	750	MB
Maximum recursion level:	24	

Using this section, you can configure limits for archive sizes and recursion levels.

After specifying the appropriate settings click on [Apply Changes](#) to make them effective.

Use the following input fields to configure limits for archives:

- [Maximum size of unpacked archive](#)

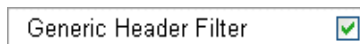
Enter the maximum size (in MB) here that should be allowed for an archive.

- [Maximum recursion level](#)

Enter the maximum number of recursion levels here that should be allowed for an archive.

3.5 Generic Header Filter

The [Generic Header Filter](#) options are invoked by clicking on the corresponding button under [Common](#):

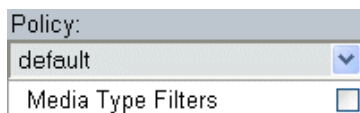


If you want to enable any of these options, make sure the checkbox on this button is also marked. The checkbox is marked by default.

After modifying the setting of this checkbox, click on [Apply Changes](#) to make the modification effective.

These are policy-dependent options, i. e. they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled [Policy](#), which is located above the [Media Type Filters](#) button:



The options are arranged under the following tab:



They are described in the upcoming section:

- [Generic Header Filter](#), see [3.5.1](#)

3.5.1 Generic Header Filter

The *Generic Header Filter* tab looks like this:

Generic Header Filter

Header Filter List - Adds, deletes or modifies HTTP, HTTPS or SMTP header

Add rule: for HTTP Request HTTP Response HTTPS Request HTTPS Response SMTP Mail

Condition Header: Condition Value: Result Header: Result Value:

Action on match: Description:

Add to all policies

Found 1 entries with "*" Number of entries per page:

Select	Rule
<input type="checkbox"/>	<input checked="" type="checkbox"/> HTTP Request <input type="checkbox"/> HTTP Response <input type="checkbox"/> HTTPS Request <input type="checkbox"/> HTTPS Response <input type="checkbox"/> SMTP <input type="checkbox"/> Mail Condition Header: X-Forwarded-For Condition Value: * Result Header: X-Forwarded-For Result Value: <input type="text"/> Action on match: <input type="text" value="Block / Drop"/> Description: <input type="text" value="Remove X-Fwd-For header"/>

Select All

There is one section on this tab:

- *Header Filter List*

It is described in the following.

Header Filter List

The *Header Filter List* section looks like this:

Header Filter List - Adds, deletes or modifies HTTP, HTTPS or SMTP header

Add rule: for HTTP Request HTTP Response HTTPS Request HTTPS Response

Condition Header: Condition Value: Result Header:

Action on match:

Add to all policies

Found 1 entries with **

Select	Rule
<input checked="" type="checkbox"/>	<input type="checkbox"/> HTTP Request <input type="checkbox"/> HTTP Response <input type="checkbox"/> HTTPS Request <input type="checkbox"/> HTTPS Response Condition Header: <input type="text" value="X-Forwarded-For"/> Condition Value: <input type="text" value="*"/> Result Header: <input type="text" value="X-Forwarded-For"/> Action on match: <input type="text" value="Block / Drop"/> <input type="button" value="v"/>

Select All

Using this section, you can configure the Generic Header Filter to delete headers and header content, add customized headers, modify existing header content, and execute any pre-defined or customized action on appropriate filtering conditions.

The filter can be configured for Web traffic using the HTTP or HTTPS protocol, as well as for e-mail traffic.

For e-mail traffic, there are two options to choose from: *SMTP* and *Mail*. If *SMTP* is selected, the configured settings will operate on the content of internal Webwasher headers such as *X-WW-From*, *X-WW-To* or *X-Client-IP*.

If *Mail* is selected, settings will operate on the content of standard e-mail headers such as *Subject*, *From* and *To*.

The filtering conditions for handling headers in this way are entered in the fields of this section. For an explanation of them, see the corresponding online help page.

On this page, examples are also provided for configuring the filter with regard to HTTP and HTTPS communication.

3.6

Generic Body Filter

The *Generic Body Filter* options are invoked by clicking on the corresponding button under *Common*:



If you want to enable any of these options, make sure the checkbox on this button is also marked. The checkbox is marked by default.

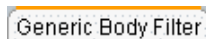
After modifying the setting of this checkbox, click on *Apply Changes* to make the modification effective.

These are policy-dependent options, i. e. they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled *Policy*, which is located above the *Media Type Filters* button:



The options are arranged under the following tab:



They are described in the upcoming section:

- *Generic Body Filter*, see [3.6.1](#)

3.6.1 Generic Body Filter

The *Generic Body Filter* tab looks like this:

Generic Body Filter

Body Filter List - Blocks content according to binary pattern rules

Add Rule:

Description:

Enabled

Applies to Media Types:
<Enter regular expression here

Applies to Transport Directions:
 Web Download
 Web Upload
 Mail

Applies to Content of Size:
 KB -
KB

Offset	Length	Operator	Byte Sequence
		Equa	
		Equa	
		Equa	
		Equa	

Clear and add expressions: 2

On match:
 WEB Block
 Classify as Please select
 Modify by
 Malware

Add Add to all policies

Other Operations:
Add File Fingerprint
Durchsuchen...

Add Add to all policies

There is this section on this tab:

- *Body Filter List*

It is described in the following.

Body Filter List

The *Body Filter List* section looks like this:

Using this section, you can configure the Generic Body Filter blocking and other actions for Web and e-mail content according to keywords, regardless of the URL it originates from.

So, you could use the Generic Body Filter, e. g. to block Win32 executables.

When configuring the filter, rules are set up of the following format:

If the 2nd byte of a file has the value of n, and the 3rd byte does not have the value of n, and within the bytes 100 to 200 a string of n can be found, then ...

The Generic Body Filter also supports case-insensitive operands by using an uppercase *I* in front of a quoted operand.

So, to block, e. g. all HTML pages encoded as *UTF-16* you can configure a rule like the following:

0-128 Contains I"<\00h\00t\00m\00\00" Or 0-128 Contains I"\00<\00h\00t\00m\00I"

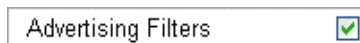
With this rule, the first expression blocks *UTF-16LE*, and the second blocks *UTF-16BE*.

The rules for filtering body content in this way and the actions that are executed when a rule matches, are entered in the fields of this section. For an explanation of them, see the corresponding online help page.

On this page, an example is also provided for configuring a body filtering rule.

3.7 Advertising Filters

The *Advertising Filters* options are invoked by clicking on the corresponding button under *Common*:



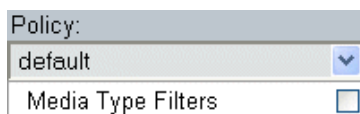
Advertising Filters

If you want to enable any of these options, make sure the checkbox on this button is also marked. The checkbox is marked by default.

After modifying the setting of this checkbox, click on *Apply Changes* to make the modification effective.

These are policy-dependent options, i. e. they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled *Policy*, which is located above the *Media Type Filters* button:



Policy:
default
Media Type Filters

The options are arranged under the following tabs:



Settings Link Filter List Dimension Filter List

They are described in the upcoming sections:

- *Settings*, see [3.7.1](#)
- *Link Filter List*, see [3.7.2](#)

- *Dimension Filter List*, see [3.7.3](#)

3.7.1 Settings

The *Settings* tab looks like this:

The screenshot shows the 'Settings' tab with the following sections:

- Link Filter** - Screens content based on information from the URL
 - Disable built-in filter list
 - Objects to be filtered:
 - Images Windows Scripts
 - Layers Frames Embedded objects
 - Forms Text links Backgrounds
- Dimension Filter** - Eliminates banner ads and objects by size
 - Objects to be filtered:
 - Images Applets Plug-ins
 - Ignore objects without specified dimensions
 - Filter objects that are located on the same server
- Pop-Up Filter** - Eliminates script-initiated pop-up browser windows
 - Also disable manually opened windows
- Script Filter** - Manages code that manipulates browsers and systems
 - Filter scripts that a Web page executes on loading
 - Filter scripts that a Web page executes on closing
 - Prevent supplementary modification of the address
 - Prevent modification of the browser's status bar
- Animation Filter** - Manages and filters animated images
 - Animated images:
 - Show only the first picture of an animation
 - Repeat animation time(s)
 - Remove all animated images
- Advertising Filter Settings** - Define rules for filtered objects
 - Replace filtered objects with:
 - a transparent image
 - another image

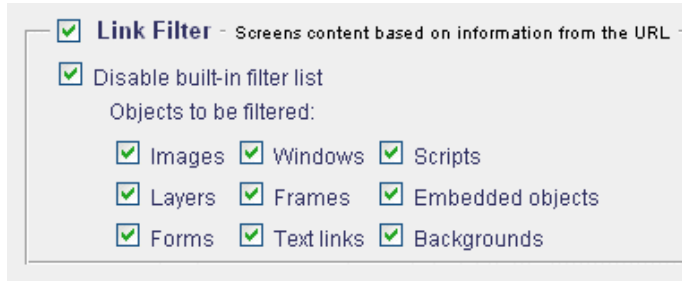
There are six sections on this tab:

- *Link Filter*
- *Dimension Filter*
- *Popup Filter*
- *Script Filter*
- *Animation Filter*
- *Advertising Filter Settings*

They are described in the following.

Link Filter

The *Link Filter* section looks like this:



Using this section, you can configure the filtering of content based on information from the URL of an object and specify different types of content that you want to have filtered.

URLs can be added for filtering to the built.in filter list or edited. The list can be accessed on the *Link Filter List* tab.

If you want to use this filter, make sure the checkbox next to the section heading is marked. The checkbox is marked by default.

All content types are also included in the filtering by default.

After modifying any of these settings, click on *Apply Changes* to make the modification effective.

Use the following checkboxes to configure the filtering of links:

- *Disable built-in filter list*

If this option is enabled, the built-in filter list is used.

Note that disabling it will severely impair the efficiency of advertisement filtering. You should only do this in case you provide a filter list of your own that you want to work with.

- *Objects to be filtered*

Mark or clear the checkboxes provided here according to the content types you want the filter to apply.

The meaning of the checkboxes is as follows:

— *Images*

Enables or disables the filtering of images.

— *Windows*

Enables or disables the filtering of windows, which are also commonly known as pop-ups.

A pop-up is a display area, usually a small window, that suddenly pops up in the foreground of the visual interface.

— *Scripts*

Enables or disables the filtering of Java scripts.

These are used on Web sites to do such things as automatically changing a formatted date on a Web page, causing a linked-to page to appear in a pop-up window, causing text or a graphic image to change during a mouse rollover, etc.

— *Layers*

Enables or disables the filtering of layers.

Web pages are often made up of positioning layers in HTML code, which may include a background as well as images or text added on top.

Layers are designed to be used with JavaScript to create dynamic pages.

— *Frames*

Enables or disables the filtering of frames.

Frames are used for independent control of multiple sections on a Web page. This is achieved by building each section as a separate HTML file and using one "master" HTML file to handle all sections.

When a user requests a Web page that uses frames, the address requested is usually that of the master file.

— *Embedded Objects*

Enables or disables the filtering of embedded objects.

Embedded objects are objects such as images, videos, Java applets that are created within another application and embedded into a document.

— *Forms*

Enables or disables the filtering of forms.

— *Text links*

Enables or disables the filtering of text links.

A text link is the grouping of linked text that, when clicked on, takes you to another page either within the same Web site, or to an entirely different Web server.

It will often open up another browser window when clicked on.

— *Backgrounds*

Enables or disables the filtering of background images.

This option only removes advertising backgrounds, but not all background images in general.

Dimension Filter

The *Dimension Filter* section looks like this:



Using this section, you can configure a filter to eliminate banner ads and objects based on their size.

To add dimensions to the Dimension Filter List go to the *Dimension Filter List* tab.

If you want to use this filter, make sure the checkbox next to the section heading is marked. The checkbox is marked by default.

After specifying the appropriate settings, click on *Apply Changes* to make them effective.

Use the following checkboxes to configure dimension filtering:

- *Objects to be filtered*

Mark or clear the checkboxes provided here according to the content types you want to the filter to apply to.

Their meaning is as follows:

— *Images*

Enables or disables the filtering of images.

— *Applets*

Enables or disables the filtering of Java applets.

These are small programs accompanying a Web page that is sent to a user. Java applets are able to perform interactive animations, instant calculations and conversions etc., without having to send a user request back to the server.

— *Plug-ins*

Enables or disables the filtering of plug-ins.

These are programs that can easily be installed and used as part of your Web browser.

- *Ignore objects without specified dimensions*

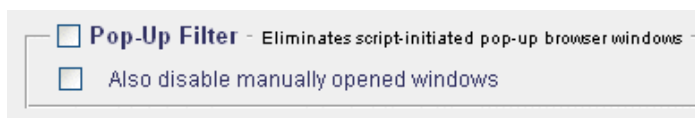
If this option is enabled, objects that have their dimensions not specified will be ignored.

- *Filter objects that are located on the same server*

If this option is enabled, objects will also be filtered if they are located on the same server. By default, such objects will go unfiltered.

Popup Filter

The *Popup Filter* section looks like this:



Using this section, you can configure a filter to eliminate script-initiated pop-up browser windows.

Furthermore, you can disable manually opened windows to ensure that pop-up windows remain closed.

If you want to use this filter, mark the checkbox next to the section heading.

After specifying this setting, you may also specify the additional setting provided here. Then click on *Apply Changes* to make your settings effective.

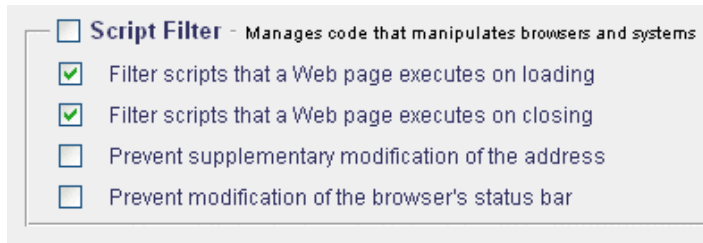
Use the following checkbox to configure the additional setting:

- *Also disable manually opened windows*

If this option is enabled, pop-ups will not be opened even if the user clicks on the corresponding link.

Script Filter

The *Script Filter* section looks like this:



Using this section, you can configure a filter to manage the code that manipulates browsers and systems.

If you want to use this filter, mark the checkbox next to the section heading.

After specifying this setting or any other setting in this section, click on *Apply Changes* to make these settings effective.

Use the following checkboxes to configure script filtering:

- *Filter scripts that a Web page executes on loading*

If this option is enabled, the filter will suppress scripts that are started automatically when a Web page is loaded.

The option is enabled by default.

- *Filter scripts that a Web page executes on closing*

If this option is enabled, the filter will suppress scripts that are started automatically when a Web page is closed.

The option is enabled by default.

- *Prevent supplementary modification of the address*

If this option is enabled, the filter will suppress special JavaScript functions that modify the IP address, i. e. that automatically transfer you from one Web page to another.

- *Prevent modification of the browser's status bar*

If this option is enabled, the filter will prevent the status bar of the browser from being modified by a Web page, i. e. scrolling text.

Animation Filter

The *Animation Filter* section looks like this:



The screenshot shows a configuration panel titled "Animation Filter" with the subtitle "Manages and filters animated images". Below the title, it says "Animated images:". There are three radio button options: "Show only the first picture of an animation" (which is selected), "Repeat animation" followed by an input field containing the number "1" and the text "time(s)", and "Remove all animated images".

Using this section, you can configure a filter to detect animated images. Animations will either be filtered completely or restricted in their execution.

If you want to use this filter, mark the checkbox next to the section heading.

After specifying this setting or any other setting in this section, click on *Apply Changes* to make these settings effective.

Use the following radio buttons to configure animation filtering:

- *Animated images*

Use the radio buttons provided here according to the measures you want the filter to take against animations:

- *Show only the first picture of an animation*

Make sure this button is checked to terminate an animation after showing the first picture.

This option is enabled by default.

- *Repeat animation . . . time(s)*

Check this button to limit repetition of the animation.

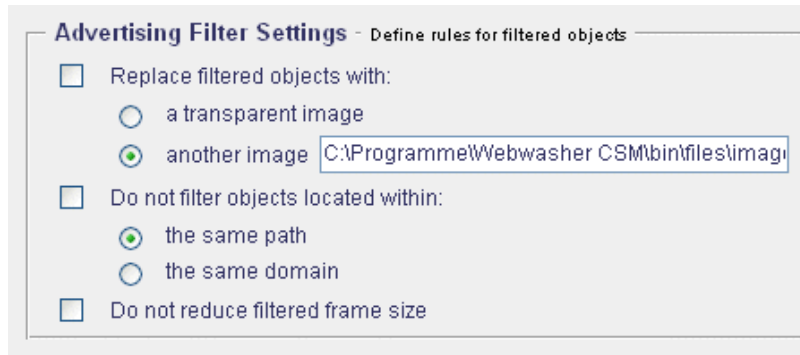
In the input field provided here enter the number of times you want an animation to repeat itself.

- *Remove all animated images*

Check this button to remove animation completely.

Advertising Filter Settings

The *Advertising Filter Settings* section looks like this:



Using this section, you can configure settings that will apply to all the filters on this tab.

After specifying the appropriate settings, click on *Apply Changes* to make them effective.

Use the following checkboxes and radio buttons to configure these settings:

- *Replace filtered objects with*

Mark this checkbox if you want to have filtered objects replaced with something.

Then check the radio buttons below to specify with what they should be replaced:

- *a transparent image*

Enable this option to replace an animated image with a transparent image.

- *another image*

Make sure this option is enabled if you want to replace an animated image with another image.

In the input field provided here, enter the path and name of the image you want to use.

The option is enabled by default. Likewise, a default image is configured to replace animations.

- *Do not filter objects located within*

Mark this checkbox if you want to exclude objects from filtering that are within the same path or domain.

Then check the radio buttons below to further specify the exclusion:

— *the same path*

Enable this option to exclude objects within the same place from filtering.

— *the same domain*

Enable this option to exclude objects within the same domain from filtering.

- *Do not reduce filtered frame size*

Mark this checkbox to prevent filtered frame sizes from being reduced.

3.7.2 Link Filter List

The *Link Filter List* tab looks like this:

The screenshot shows the 'Link Filter List' tab in a settings window. At the top, there are three tabs: 'Settings', 'Link Filter List', and 'Dimension Filter List'. The 'Link Filter List' tab is active. Below the tabs, the title is 'Link Filter List - Screens content based on information about the URL'. There is a search icon in the top right corner. The main area contains a form for adding new URLs. It has a dropdown menu set to 'String' and a text input field. Below the input field are two checkboxes: 'deactivate' and 'do not filter'. There are two buttons: 'Add to Link Filter List' and 'Add to all policies'. Below this form, it says 'Found 1 entries with ""'. To the right, there is a 'Number of entries per page:' dropdown set to '10'. Below this is a table with a 'Select' column and a 'URL' column. The table has one row with a checked checkbox in the 'Select' column and the URL 'example/beispiel' in the 'URL' column. To the right of the URL are two checkboxes: 'deactivate' (checked) and 'do not filter'. At the bottom of the table, there are two buttons: 'Select All' (checked) and 'Delete Selected'.

There is one section on this tab:

- *Link Filter List*

It is described in the following.

Link Filter List

The *Link Filter List* section looks like this:

Link Filter List - Screens content based on information about the URL

Add new URL:
(Format: /unwanted-dir/a*.html)

deactivate do not filter

Add to all policies

Found 1 entries with **

Select	URL
<input type="checkbox"/>	example/beis?iel <input checked="" type="checkbox"/> deactivate <input type="checkbox"/>

Select All

Using this section, you can add URLs to the Link Filter List and edit them.

To do this, use the area labeled:

- *Add new URL*

Select *String* or *International Domain Name* from the first of the drop-down lists provided here.

In the input field next to it, enter a string to specify the object using shell expressions.

Select *International Domain Name* if you want to enter non-ASCII characters and the string should be used for the domain part of an URL.

In some countries like Germany, Sweden or Japan, domain names with non-ASCII characters are allowed. The IDNA (International Domain Names in Applications) standard describes how a Web browser should convert such a domain name into pure ASCII notation used, e. g. by DNS.

Webwasher uses the pure ASCII notation as well, therefore all IDN strings must be converted. This is done automatically when you select *International Domain Name* and enter a string with non-ASCII characters.

Note that you can not use shell expressions with IDN strings.

Furthermore, use the following items when adding a new entry to the list:

- *deactivate*

Enable this option to insert a new URL in the list that will not yet be used for filtering, however.

— *do not filter*

Enable this option to exclude the URL you entered above from filtering.

— *Add to Link Filter List*

After specifying the information for a URL, click on this button to add it to the list.

This addition will be valid only under the policy you are currently configuring.

To add a URL to the list for all policies, mark the checkbox labeled *Add to all policies* before clicking on the button.

If a URL or shell expression that was configured under another policy is already in the list, the setting of the *Add to all policies* checkbox will have no effect.

The Link Filter List is displayed at the bottom of this section.

To display only a particular number of list entries at a time, type this number in the input field labeled *Number of entries per page* and enter it using the *Enter* key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To sort the list in ascending or descending order, click on the symbol next to the *URL* column heading.

To edit an entry, type the appropriate text in the corresponding input field and mark or clear the *deactivate* and *do not filter* checkboxes in the same line.

Then click on *Apply Changes* to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- *Filter*

Type a filter expression in this input field and enter it using the *Enter* key of your keyboard. The list will then display only entries matching the filter.

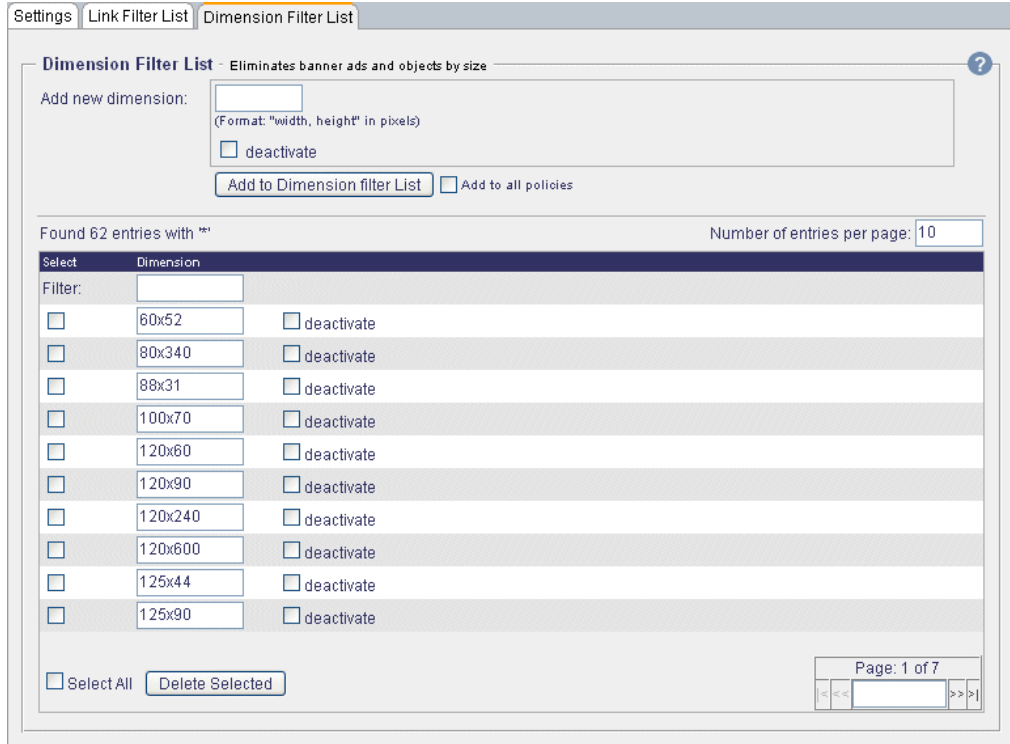
- *Delete Selected*

Select the entry you wish to delete by marking the *Select* checkbox next to it and click on this button. You can delete more than one entry in one go.

To delete all entries, mark the *Select all* checkbox and click on this button.

3.7.3 Dimension Filter List

The *Dimension Filter List* tab looks like this:



There is this one section on this tab:

- *Dimension Filter List*

It is described in the following.

Dimension Filter List

The *Dimension Filter List* section looks like this:

Dimension Filter List - Eliminates banner ads and objects by size

Add new dimension:
 (Format: "width, height" in pixels)

deactivate

Add to all policies

Found 62 entries with '*'

Select	Dimension	
<input type="checkbox"/>	<input type="text" value="60x52"/>	<input type="checkbox"/> deactivate
<input type="checkbox"/>	<input type="text" value="80x340"/>	<input type="checkbox"/> deactivate
<input type="checkbox"/>	<input type="text" value="88x31"/>	<input type="checkbox"/> deactivate
<input type="checkbox"/>	<input type="text" value="100x70"/>	<input type="checkbox"/> deactivate
<input type="checkbox"/>	<input type="text" value="120x60"/>	<input type="checkbox"/> deactivate
<input type="checkbox"/>	<input type="text" value="120x90"/>	<input type="checkbox"/> deactivate
<input type="checkbox"/>	<input type="text" value="120x240"/>	<input type="checkbox"/> deactivate
<input type="checkbox"/>	<input type="text" value="120x600"/>	<input type="checkbox"/> deactivate
<input type="checkbox"/>	<input type="text" value="125x44"/>	<input type="checkbox"/> deactivate
<input type="checkbox"/>	<input type="text" value="125x90"/>	<input type="checkbox"/> deactivate

Select All

Using this section, you can add dimension settings to the Dimension Filter List and edit them.

These can be used for filtering images, applets and plug-ins.

To do this, use the area labeled:

- *Add new dimension*

In the input field provided here, enter a pair of pixel values to specify the height and width of an object that should be filtered, e. g. *60x52*.

Furthermore, use the following item when adding dimension settings to the list:

— *deactivate*

If this option is enabled the corresponding dimension settings will be added to the list, but not yet used for filtering.

— *Add to Dimension Filter List*

After specifying the dimensions settings in the way described above, click on this button to add them to the list.

This addition will be valid only under the policy you are currently configuring.

To add dimensions to the list for all policies, mark the checkbox labeled *Add to all policies* before clicking on the button.

If dimension settings that were configured under another policy are already in the list, the setting of the *Add to all policies* checkbox will have no effect.

The Dimension Filter List is displayed at the bottom of this section.

To display only a particular number of list entries at a time, type this number in the input field labeled *Number of entries per page* and enter it using the *Enter* key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To edit an entry, type the appropriate pixel values in the corresponding input field and mark or clear the *deactivate* checkbox in the same line.

Then click on *Apply Changes* to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- *Filter*

Type a filter expression in this input field and enter it using the *Enter* key of your keyboard. The list will then display only entries matching the filter.

- *Delete Selected*

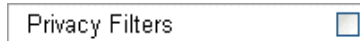
Select the entry you wish to delete by marking the *Select* checkbox next to it and click on this button. You can delete more than one entry in one go.

To delete all entries, mark the *Select all* checkbox and click on this button.

3.8

Privacy Filters

The *Privacy Filters* options are invoked by clicking on the corresponding button under *Common*:

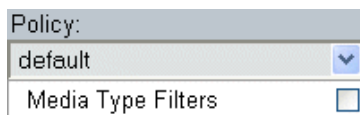


If you want to enable any of these options, mark the checkbox that is on this button.

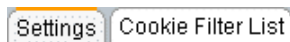
Then click on *Apply Changes* to make this setting effective.

These are policy-dependent options, i. e. they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled *Policy*, which is located above the *Media Type Filters* button:



The options are arranged under the following tabs:

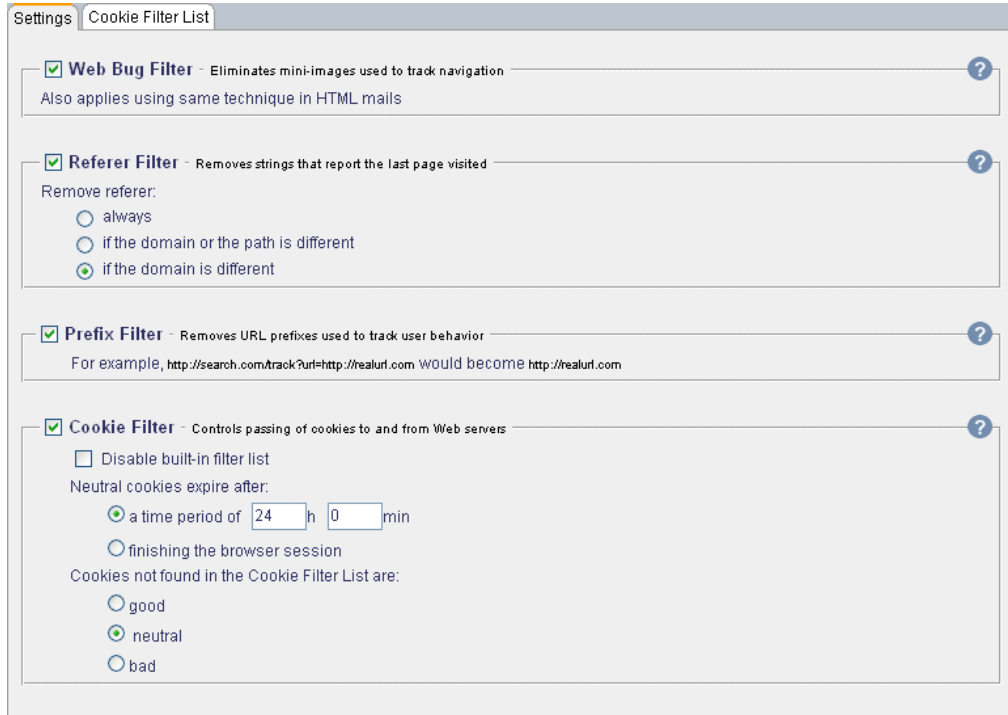


They are described in the upcoming sections:

- *Settings*, see [3.8.1](#)
- *Cookie Filter List*, see [3.8.2](#)

3.8.1 Settings

The *Settings* tab looks like this:



There are four sections on this tab:

- *Web Bug Filter*
- *Referer Filter*
- *Prefix Filter*
- *Cookie Filter*

They are described in the following.

Web Bug Filter

The *Web Bug Filter* section looks like this:



Using this section, you can configure a filter to eliminate Web bugs.

These are also known as clear GIFs or Web beacons. They are usually 1 pixel x 1 pixel mini-images in size and are used to track user navigation behavior on Web sites and in e-mail to see if an e-mail was opened by the recipient.

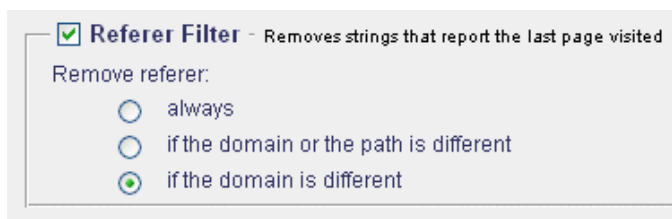
The filter is also applied to the same technique used in HTML messages.

If you want to use this filter, make sure the checkbox next to the section heading is marked. The checkbox is marked by default.

After modifying this setting, click on [Apply Changes](#) to make the modification effective.

Referer Filter

The [Referer Filter](#) section looks like this:



Referer Filter - Removes strings that report the last page visited

Remove referer:

- always
- if the domain or the path is different
- if the domain is different

Using this section, you can configure a filter to remove referer strings that report the last page visited by a user.

If you want to use this filter, make sure the checkbox next to the section heading is marked. The checkbox is marked by default.

After modifying this setting or any other setting in this section, click on [Apply Changes](#) to make the modification effective.

To configure the filtering of referer strings, use the radio buttons of the area labeled:

- [Remove referer](#)

Check or uncheck one of these three radio buttons as needed:

— [always](#)

If this option is enabled a referer is always removed regardless of where the user in question came from.

— [if the domain or the path is different](#)

If this option is enabled a referer is removed if the user came from a different path or URL.

It leaves the referer unaffected if you the user moves through the same or subsequent path.

This option may be enabled if user movement should be hidden, but there are services that rely on a referer to work properly.

— *if the domain is different*

If this option is enabled a referer is removed in case the user came from a different Web site.

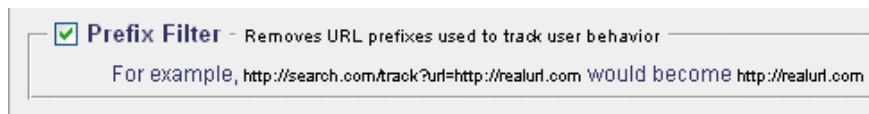
It leaves the referer unaffected if the user moves through the same Web site.

This allows the Webmaster to track user movement through this Web site. The information may be useful for adjusting or optimizing the navigational structure of the site.

As well, some services such as online banking may need a referer to work properly.

Prefix Filter

The *Prefix Filter* section looks like this:



Using this section, you can configure a filter to remove all prefixes from URLs that are used by some sites to track user behavior.

If you want to use this filter, make sure the checkbox next to the section heading is marked. The checkbox is marked by default.

After modifying this setting, click on *Apply Changes* to make the modification effective.

Cookie Filter

The *Cookie Filter* section looks like this:

Using this section, you can configure a filter to block bad cookies.

You can set the life span for neutral cookies or let them expire after finishing the browser session.

The Cookie Filter controls the data stream between users and the Web in both directions, a requirement for efficient filtering. Transmitted cookies coming in on the Web server, in addition to those from the browser, are controlled by Webwasher.

The distinction between the good, and thus necessary cookies, and the bad cookies that invade privacy is carried out by Webwasher using an algorithm and the built-in filter list depending on the URL of a cookie.

To add and edit cookies on this list, go to the *Cookie Filter List* tab.

If you want to use this filter, make sure the checkbox next to the section heading is marked. The checkbox is marked by default.

After modifying any of these settings, click on *Apply Changes* to make the modification effective.

Use the following items to configure cookie filtering:

- *Disable built-in filter list*

If this option is enabled the built-in filter list is used. The option is disabled by default.

- *Neutral cookies expire after*

Use the radio buttons and input fields provided here in the following way:

— *a time period of . . . h . . . min*

Make sure this radio button is checked if you want to configure a life span for neutral cookies. The radio button is checked by default.

Enter the appropriate time periods (in hours and minutes) in the input fields provided here. The default value is 24 hours.

— *finishing the browser session*

Check this radio button to let neutral cookies expire when sessions are ended.

A pop-up is a display area, usually a small window, that suddenly pops up in the foreground of the visual interface.

• *Cookies not found in the filter list are*

Use the radio buttons provided to configure a default classification for cookies:

— *good*

Check this radio button to classify unknown cookies as good.

— *neutral*

Check this radio button to classify unknown cookies as neutral.

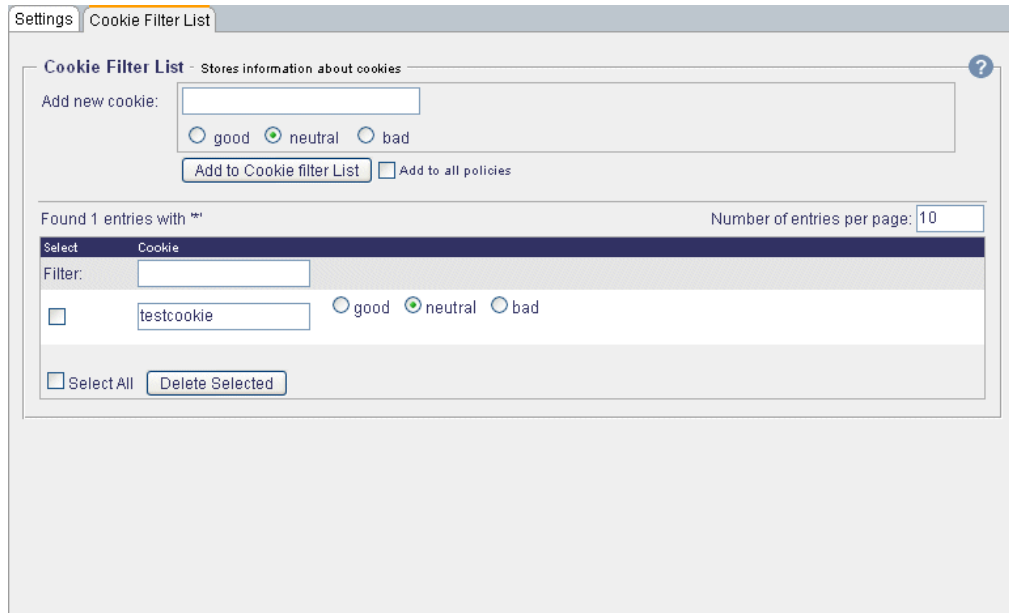
Unknown cookies are classified so by default.

— *bad*

Check this radio button to classify unknown cookies as bad.

3.8.2 Cookie Filter List

The *Cookie Filter List* tab looks like this:



The screenshot shows the 'Cookie Filter List' tab in a settings application. At the top, there are tabs for 'Settings' and 'Cookie Filter List'. Below the tabs, the title 'Cookie Filter List - Stores information about cookies' is displayed with a help icon. The main area contains an 'Add new cookie:' section with a text input field, radio buttons for 'good', 'neutral' (selected), and 'bad', and two buttons: 'Add to Cookie filter List' and 'Add to all policies'. Below this, a search bar shows 'Found 1 entries with *'. To the right, 'Number of entries per page: 10' is shown. A table with columns 'Select' and 'Cookie' contains one entry: a checkbox, a text input with 'testcookie', and radio buttons for 'good', 'neutral' (selected), and 'bad'. At the bottom of the table area, there are 'Select All' and 'Delete Selected' buttons.

There is one section on the tab:

- *Cookie Filter List*

It is described in the following.

Cookie Filter List

The *Cookie Filter List* section looks like this:

The screenshot shows the 'Cookie Filter List' configuration window. At the top, it says 'Cookie Filter List - Stores information about cookies'. Below this is an 'Add new cookie:' section with an input field, three radio buttons labeled 'good', 'neutral', and 'bad' (with 'neutral' selected), and two buttons: 'Add to Cookie filter List' and 'Add to all policies'. Below that, it says 'Found 1 entries with **'. There is a table with two columns: 'Select' and 'Cookie'. The table contains one entry: a checkbox in the 'Select' column and 'testcookie' in the 'Cookie' column. To the right of the table are three radio buttons labeled 'good', 'neutral', and 'bad' (with 'neutral' selected). At the bottom of the table area are two buttons: 'Select All' and 'Delete Selected'.

Using this section, you can add entries to the Cookie Filter List and edit them.

Shell expressions in this list will be compared to the domain where the cookie was sent from or will be sent to, in order to determine whether the cookie is good, neutral or bad. Good cookies can pass, bad cookies are filtered out and neutral cookies will vanish after the configured life span.

To add a cookie to the list, use the area labeled:

- *Add new cookie*

In the input field provided here enter the cookie.

Then classify it by checking of one of these three radio buttons:

— *good – neutral – bad*

The *neutral* button is checked by default.

— *Add to Cookie Filter List*

After specifying a cookie and classifying it, click on this button to add it to the list.

This addition will be valid only under the policy you are currently configuring.

To add a cookie to the list for all policies, mark the checkbox labeled *Add to all policies* before clicking on the button.

If a cookie that was configured under another policy is already in the list, the setting of the *Add to all policies* checkbox will have no effect.

The Cookie Filter List is displayed at the bottom of this section.

To display only a particular number of list entries at a time, type this number in the input field labeled *Number of entries per page* and enter it using the *Enter* key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To edit an entry, type the appropriate text in the input field of the cookie, and check or uncheck the *good*, *neutral* or *bad* button in the same line.

Then click on *Apply Changes* to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- *Filter*

Type a filter expression in this input field and enter it using the *Enter* key of your keyboard. The list will then display only entries matching the filter.

- *Delete Selected*

Select the entry you wish to delete by marking the *Select* checkbox next to it and click on this button. You can delete more than one entry in one go.

To delete all entries, mark the *Select all* checkbox and click on this button.

3.9

Text Categorization

The *Text Categorization* options are invoked by clicking on the corresponding button under *Common*:

 Text Categorization

If you want to enable any of these options, mark the checkbox that is on this button.

Then click on *Apply Changes* to make this setting effective.

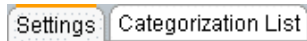
These are policy-dependent options, i. e. they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled *Policy*, which is located above the *Media Type Filters* button:



A screenshot showing a 'Policy:' label above a dropdown menu with 'default' selected. Below it is a 'Media Type Filters' button with a small square icon.

The options are arranged under the following tabs:



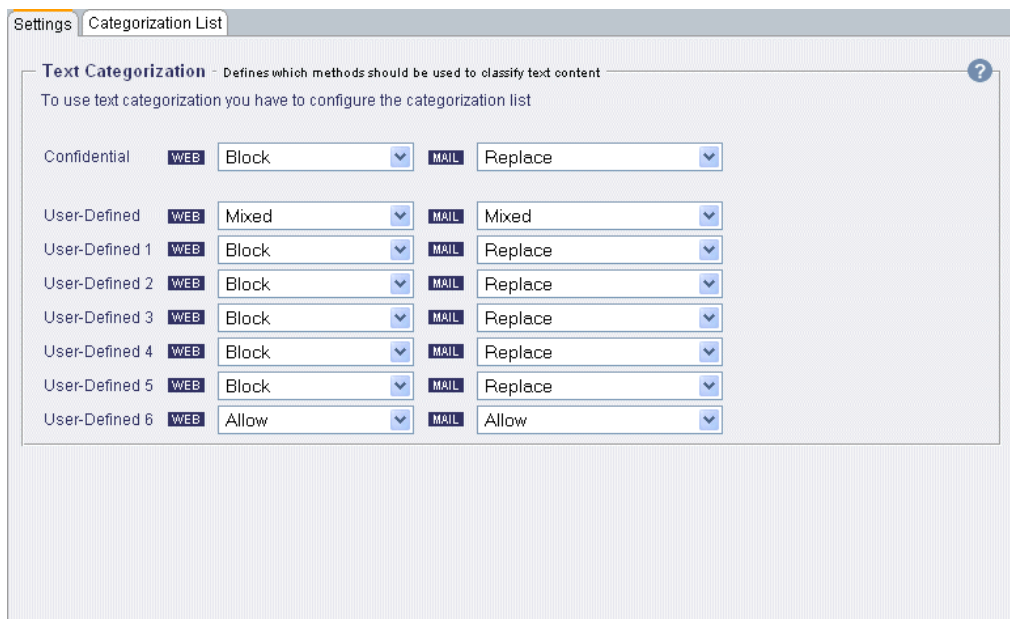
A screenshot showing two tabs: 'Settings' (highlighted with an orange bar) and 'Categorization List'.

They are described in the upcoming sections:

- *Settings*, see [3.9.1](#)
- *Categorization List*, see [3.9.2](#)

3.9.1 Settings

The *Settings* tab looks like this:



A screenshot of the 'Settings' tab in a web interface. The 'Categorization List' sub-tab is active. The main section is titled 'Text Categorization' with a subtitle 'Defines which methods should be used to classify text content'. Below this, there is a table of settings for different content categories. Each row has a category name, a 'WEB' method dropdown, and a 'MAIL' method dropdown.

Category	WEB Method	MAIL Method
Confidential	Block	Replace
User-Defined	Mixed	Mixed
User-Defined 1	Block	Replace
User-Defined 2	Block	Replace
User-Defined 3	Block	Replace
User-Defined 4	Block	Replace
User-Defined 5	Block	Replace
User-Defined 6	Allow	Allow

There is one section on this tab:

- *Text Categorization*

It is described in the following.

Text Categorization

The *Text Categorization* section looks like this:

Category	WEB Action	MAIL Action
Confidential	Block	Replace
User-Defined	Mixed	Mixed
User-Defined 1	Block	Replace
User-Defined 2	Block	Replace
User-Defined 3	Block	Replace
User-Defined 4	Block	Replace
User-Defined 5	Block	Replace
User-Defined 6	Allow	Allow

Using the text categorization filter you can specify single keywords and combinations of words and filter office documents and e-mail attachments containing these words.

In this section, you configure the actions that should be taken whenever the text categorization filter matches. You can configure different actions for particular categories of documents.

Furthermore, you can configure different actions for Web and e-mail traffic.

A confidential category is provided here for a start. Apart from this, you can configure actions for up to six categories of your own.

The rules for the keywords and combinations that should be filtered are configured and listed on the *Categorization List* tab.

If you want to configure actions for text categorization, select them from the appropriate drop-down lists.

Then click on *Apply Changes* to make your settings effective.

Select actions for Web and e-mail traffic from the following lists:

- *Confidential*

Select actions for documents falling into the confidential category here.

- *User-Defined, User Defined 1 , etc.*

Select actions for documents falling into any of your own categories here.

3.9.2 Categorization List

The *Categorization List* tab looks like this:

Settings | Categorization List

Text Categorization List - Uses Boolean Logic to define content categorization rules

Add Rule: AND AND NOT
 more than times per words

Select one or more categories to apply to the above rule:

Category 1:

Category 2:

Category 3:

Add to all policies

Found 1 entries with "x" Number of entries per page:

Select	Rule
<input type="checkbox"/>	<input type="text" value="Bahamas"/> AND <input type="text" value="Maledives"/> AND NOT <input type="text" value="work"/> Categories: <input type="text" value="User-Defined 1"/> <input type="text" value="Please select"/> <input type="text" value="Please select"/> <input type="checkbox"/> Deactivate

Select All

There is one section on this tab:

- *Text Categorization List*

It is described in the following.

Text Categorization List

The *Text Categorization List* section looks like this:

Text Categorization List - Uses Boolean Logic to define content categorization rules

Add Rule: [] AND [] AND NOT []

[] more than [] times per [] words

Select one or more categories to apply to the above rule:

Category 1: Please select

Category 2: Please select

Category 3: Please select

Create Rule Add to all policies

Found 1 entries with **

Select	Rule
<input type="checkbox"/>	Bahamas AND Maledives AND NOT work Categories: User-Defined 1 Please select Please select

Select All

Using the text categorization filter you can specify single keywords and combinations of words and filter office documents and e-mail attachments containing these words.

In this section, you can configure rules for the keywords and combinations of keywords that should be filtered and add them to the Text Categorization List.

To add a text categorization rule to the list, use the area labeled:

- *Add rule*

Use the following items to configure a rule and add it to the list:

— *[term 1] AND [term 2] AND NOT [term 3]*

Make sure the radio button in this line is checked if you want to configure a rule according to this method, which is one of two provided here.

This method uses Boolean logic to determine the placement of words in an office document or e-mail message. It is enabled by default.

In the input fields, enter the words or word combinations you want to filter, e. g. *Bahamas*, *Maledives*, *work* to set up a rule like the following:

Bahamas AND Maledives AND NOT work

— *[term 1] more than [term 2] times per [term 3] words*

Check the radio button in this line to configure a rule according to the second method provided here.

It is based on counting how often a particular word or combination appears in the text body of an office document or an e-mail message.

In the input fields, enter the word or word combination you want to filter, e. g. *money*, *3*, *10* to set up a rule like the following:

money more than 3 times per 10 words

— *Select one or more categories to apply to the above rule*

From the drop-down lists provided here select one or more categories. The rule configured above will be applied within these categories.

— *Create Rule*

After setting up a text categorization rule, click on this button to add it to the list.

This addition will be valid only under the policy you are currently configuring.

To add a rule to the list for all policies, mark the checkbox labeled *Add to all policies* before clicking on the button.

The Text Categorization List is displayed at the bottom of this section.

To display only a particular number of list entries at a time, type this number in the input field labeled *Number of entries per page* and enter it using the *Enter* key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To edit an entry, type the appropriate text in the input field of the rule.

Enable or disable a rule by marking or clearing the *Deactivate* checkbox in the corresponding line.

Then click on *Apply Changes* to make these settings effective. You can edit more than one list entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- *Filter*

Type a filter expression in this input field and enter it using the *Enter* key of your keyboard. The list will then display only entries matching the filter.

- *Delete Selected*

Select the entry you wish to delete by marking the *Select* checkbox next to it and click on this button. You can delete more than one entry in one go.

To delete all entries, mark the *Select all* checkbox and click on this button.

3.10

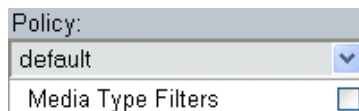
White List

The *White List* options are invoked by clicking on the corresponding button under *Common*:


 A rectangular button with the text "White List" inside.

These are policy-dependent options, i. e. they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled *Policy*, which is located above the *Media Type Filters* button:


 A screenshot of a web interface showing a "Policy:" label above a dropdown menu. The dropdown menu is open, showing "default" as the selected option with a blue downward arrow. Below the dropdown is a checkbox labeled "Media Type Filters" which is currently unchecked.

The options are arranged under the following tab:

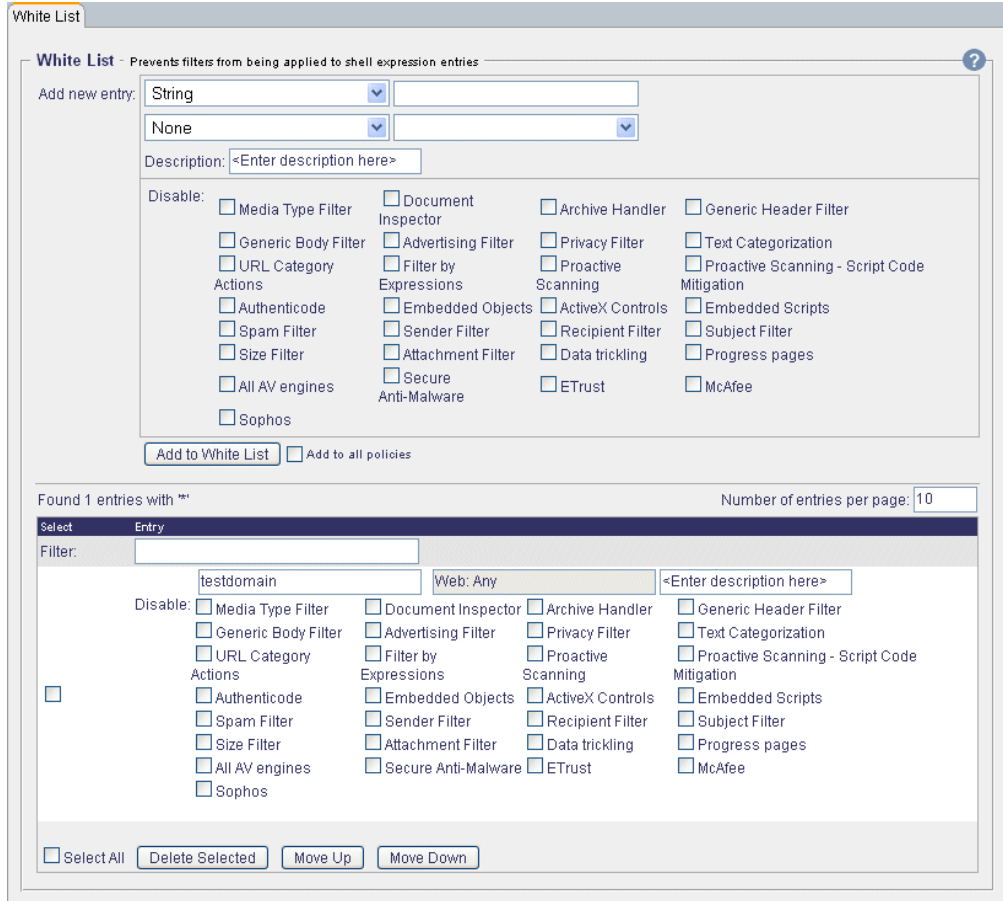

 A tab labeled "White List" with a small orange highlight on its top-left corner.

They are described in the upcoming section:

- *White List*, see [3.10.1](#)

3.10.1 White List

The *White List* tab looks like this:



There is one section on this tab:

- *White List*

It is described in the following.

White List

The *White List* section looks like this:

White List - Prevents filters from being applied to shell expression entries

Add new entry: String [v] []

None [v] [v]

Description: <Enter description here>

Disable:

- Media Type Filter
- Document Inspector
- Archive Handler
- Generic Body Filter
- Advertising Filter
- Privacy Filter
- URL Category Actions
- Filter by Expressions
- Proactive Scanning
- Authenticode
- Embedded Objects
- ActiveX Controls
- Spam Filter
- Sender Filter
- Recipient Filter
- Size Filter
- Attachment Filter
- Data trickling
- All AV engines
- Secure Anti-Malware
- ETrust
- Sophos

[Add to White List] Add to all policies

Found 1 entries with **

Select	Entry
<input type="checkbox"/>	Filter: [] testdomain [] Web: Any []

Disable:

- Media Type Filter
- Document Inspector
- Advertising Filter
- Filter by Expressions
- Embedded Objects
- Sender Filter
- Attachment Filter
- Secure Anti-Malware
- Sophos

[Select All] [Delete Selected] [Move Up] [Move Down]

Using this section, you can add an object to the White List and exclude it from the application of particular Webwasher filters.

The objects can be specified using shell expressions. Furthermore, you can specify the type of object you would like to exclude from filtering, e. g. *Web*, *E-Mail*, *Media Type*, etc.

To specify exactly what the filters are that the object in question should be excluded from, there is a list of filters provided here, where you can disable and enable filters according to your requirements.

To add an object to the white list, use the area labeled:

- *Add new entry*

Select *String* or *International Domain Name* from the first of the drop-down lists provided here.

In the input field next to it, enter a string to specify the object using shell expressions.

To specify the object type, select *Web*, *E-Mail*, *Archive*, *Media Type*, *Embedded Object*, or *Header* from the drop-down list below the first one.

You can further specify the object type by selecting a value from the drop-down list to the right. So, e. g. for *Embedded Object* you can further specify *Any Type*, *ActiveX* or *Link*.

Furthermore, use the following items when adding a new entry to the list:

- *Description*

Input in this field is optional. You may enter a description of the media type here.

- *Disable*

In the list of filters provided here, specify those that you want to exclude the object in question from. To do this mark the corresponding checkboxes.

If you would, e. g., like to allow pop-up windows from an online banking Web site, enter the domain name of the site in the input field provided above and disable the Advertising Filter.

- *Add to White List*

After specifying the information for an object, click on this button to add it to the list.

This addition will be valid only under the policy you are currently configuring.

To add an object to the white list for all policies, mark the checkbox labeled *Add to all policies* before clicking on the button.

The White List is displayed at the bottom of this section.

To display only a particular number of list entries at a time, type this number in the input field labeled *Number of entries per page* and enter it using the *Enter* key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To sort the list in ascending or descending order, click on the symbol next to the *Media Type* or *Description* column heading.

To edit an entry, type the appropriate text in the input field for the object name or its description and enable or disable the filters as needed.

Then click on *Apply Changes* to make these settings effective. You can edit more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- *Filter*

Type a filter expression in this input field and enter it using the *Enter* key of your keyboard. The list will then display only entries matching the filter.

- *Delete Selected*

Select the entry you wish to delete by marking the *Select* checkbox next to it and click on this button. You can delete more than one entry in one go.

To delete all entries, mark the *Select all* checkbox and click on this button.

- *Move Up, Move Down*

Select the entry you wish to move by marking the *Select* checkbox next to it and click on either of these buttons, depending on where you want to move the entry.

The position an entry takes in the list is important since whenever there is more than one entry in the list containing information on a particular object, the entry that is first in the list wins.

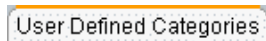
3.11

User Defined Categories

The *User Defined Categories* options are invoked by clicking on the corresponding button under *Common*:



The options are arranged under the following tab:



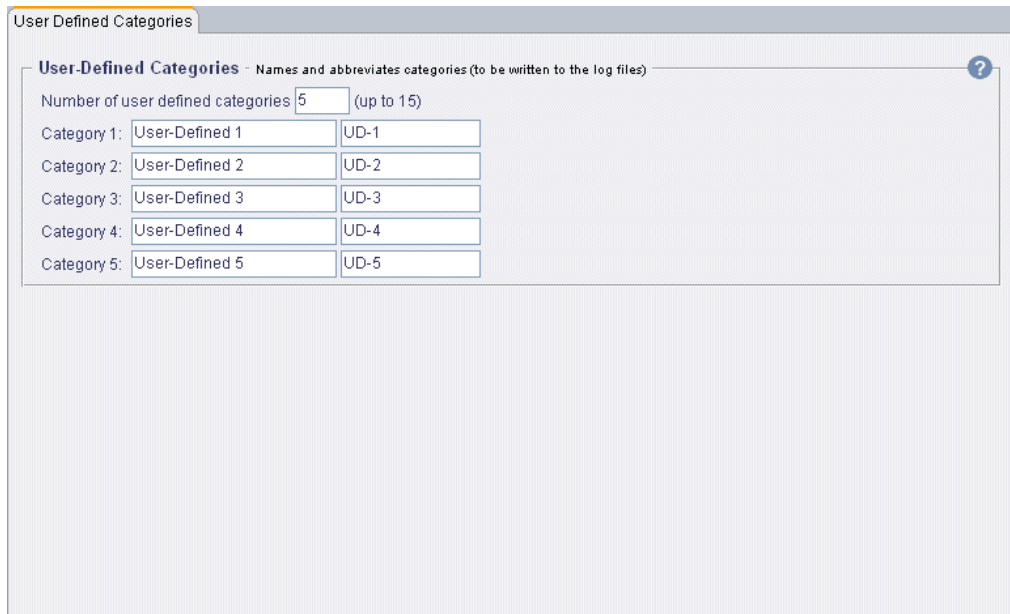
They are described in the upcoming section:

- *User Defined Categories*, see [3.11.1](#)

3.11.1

User Defined Categories

The *User Defined Categories* tab looks like this:



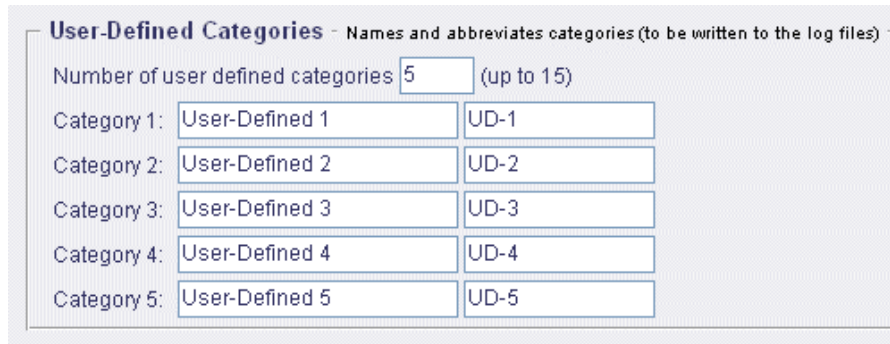
There is one section on this tab:

- *User Defined Categories*

It is described in the following.

User Defined Categories

The *User Defined Categories* section looks like this:



User-Defined Categories - Names and abbreviates categories (to be written to the log files)		
Number of user defined categories <input type="text" value="5"/> (up to 15)		
Category 1:	<input type="text" value="User-Defined 1"/>	<input type="text" value="UD-1"/>
Category 2:	<input type="text" value="User-Defined 2"/>	<input type="text" value="UD-2"/>
Category 3:	<input type="text" value="User-Defined 3"/>	<input type="text" value="UD-3"/>
Category 4:	<input type="text" value="User-Defined 4"/>	<input type="text" value="UD-4"/>
Category 5:	<input type="text" value="User-Defined 5"/>	<input type="text" value="UD-5"/>

Using this section, you can configure your own categories for URL classification with names and abbreviated name formats. You can configure up to 15 categories this way.

The abbreviated format is needed for two purposes: the log files and the X-Attribute header. The X-Attribute header is a type of REQMOD/RESPMOD header, and is a compatibility setting used to simplify the cooperation between the ICAP server and client.

Note that after changing an abbreviated name (all the possible values of the X-Attribute header will be sent in the OPTIONS response), ICAP clients may run into problems until the next OPTIONS request if they rely on previous OPTIONS responses.

The categories that you configure here will be shown on the *Category Actions* tab under *URL Filter > Category Actions*, where you can configure actions, e. g. *Block, Block, log and notify, Allow* etc. for these categories.

After specifying the appropriate settings, click on *Apply Changes* to make them effective.

Use the following items to configure your own categories:

- *Number of user defined categories*

In the input field provided here, enter the number of categories you want to configure. The maximum number is 15 (Default : 5).

Then click on *Apply Changes* for the first time. You need to click on this button a second time after specifying the settings for the individual categories.

The list of category input fields will then be enlarged or reduced according to the number you entered.

- *Category 1 to Category n*

In the input fields provided here, enter the category names you want to use and the abbreviated formats of these names.

3.12

Media Type Catalog

The *Media Type Catalog* options are invoked by clicking on the corresponding button under *Common*:

Media Type Catalog

The options are arranged under the following tab:

Media Type Catalog

They are described in the upcoming section:

- *Media Type Catalog*, see [3.12.1](#)

3.12.1 Media Type Catalog

The *Media Type Catalog* tab looks like this:

Media Type Catalog - Defines media types and how to recognize them

Add or modify Media Type:

File Extensions:

Options:

Magic bytes are necessary

Magic bytes are ambiguous

Magic Bytes - This table contains sequences for recognizing this media type

Offset	Magic Bytes
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Found 129 entries with ** Number of entries per page:

Select	Media Type	
<input type="checkbox"/>	application/ace	[-> view details or edit]
<input type="checkbox"/>	application/arc	[-> view details or edit]
<input type="checkbox"/>	application/arj	[-> view details or edit]
<input type="checkbox"/>	application/basic-source	[-> view details or edit]
<input type="checkbox"/>	application/batch	[-> view details or edit]
<input type="checkbox"/>	application/blakhole	[-> view details or edit]
<input type="checkbox"/>	application/cab	[-> view details or edit]
<input type="checkbox"/>	application/cmd	[-> view details or edit]
<input type="checkbox"/>	application/cpio	[-> view details or edit]
<input type="checkbox"/>	application/executable	[-> view details or edit]

Select All

Page: 1 of 13

There is one section on this tab:

- *Media Type Catalog*

It is described in the following.

Media Type Catalog

The *Media Type Catalog* section looks like this:

Media Type Catalog - Defines media types and how to recognize them

Add or modify Media Type:

File Extensions:

Options:

- Magic bytes are necessary
- Magic bytes are ambiguous

Magic Bytes - This table contains sequences for recognizing this media type

Offset	Magic Bytes
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

Found 129 entries with **

Select	Media Type
<input type="checkbox"/>	application/ace
<input type="checkbox"/>	application/arc
<input type="checkbox"/>	application/arj
<input type="checkbox"/>	application/basic-source
<input type="checkbox"/>	application/batch
<input type="checkbox"/>	application/blakhole
<input type="checkbox"/>	application/cab
<input type="checkbox"/>	application/cmd
<input type="checkbox"/>	application/cpio
<input type="checkbox"/>	application/executable

Filter:

Select All

Using this section, you can add a media type to the Media Type Catalog.

A media (content) type is a general category of data content, such as an application, audio content, a text message, an image, a video stream, etc.

The media type tells the application that receives the data what kind of application is needed to process the content, e. g. Real Audio is to play the audio content for a user.

Each of these media types also have subtypes, e. g. the text media type has four subtypes: plain, rich text, enriched, and tab-separated values.

You can also specify how a media type should be recognized by the particular magic byte sequences of the files belonging to it.

To add a media type to the catalog, use the area labeled:

- *Add or modify Media Type*

In the upmost input field provided here, enter the media type you want to add to the catalog.

Furthermore, use the following items when adding a media type to the catalog:

- *File Extensions*

In the input fields provided here, specify up to three extensions that files of the media type in question may have. So, e. g. the media type *image/jpeg* can have *jpg* or *jpeg* as extensions.

- *Options*

Configure the following options by marking the checkboxes provided for each of them:

- *Magic bytes are necessary*

If this option is enabled, a file that does not match the magic bytes sequences specified for its media type will be affected by the action, e. g. *Block*, configured for the Media Type Filter.

The corresponding setting is labeled *Non-rectifiable media types with magic bytes mismatch* and can be configured in the *Media Type Filter* section of the *Actions* tab under *Common > Media Type Filters*.

- *Magic bytes are ambiguous*

If this option is enabled, a file that does not match the magic bytes sequences specified for its media type will be affected by the action, e. g. *Block*, configured for the Media Type Filter.

It will, however, not be affected if several magic byte sequence were specified and one of them matches.

For the corresponding setting, see the description of the *Magic bytes are necessary* option above.

— *Magic Bytes*

In the input fields provided here, enter up to five magic byte sequences and their offsets to identify a media type:

Offset

In the input fields of this column enter the offset values for the magic byte sequences.

Magic Bytes

In the input fields of this column enter the values for the magic byte sequences themselves.

— *Add/Modify*

After specifying the information for a media type, click on this button to add it to catalog.

The list of the Media Type Catalog is displayed at the bottom of this section.

To display only a particular number of list entries at a time, type this number in the input field labeled *Number of entries per page* and enter it using the *Enter* key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To view the details of an entry or modify them, click on the *view details or edit* link in the same line. This will display the information that was configured for it in the input fields and checkboxes of the upper part of the section, where you can modify it according to your requirements.

After modifying this information, click on the *Add/Modify* button to make the modification effective. You can modify more than one entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- *Filter*

Type a filter expression in the input field of the *Media Type* column at the top of the list and enter it using the *Enter* key of your keyboard. The list will then display only entries matching the filter.

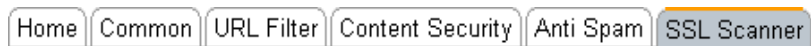
- *Delete Selected*

Select the entry you wish to delete by marking the *Select* checkbox next to it and click on this button. You can delete more than one entry in one go.

To delete all entries, mark the *Select all* checkbox and click on this button.

SSL Scanner

The features that are described in this chapter are accessible over the *SSL Scanner* tab of the Web interface:



These features allow you to configure the filtering of SSL-encrypted traffic, thus protecting your network against viruses and other malicious content that may be hidden behind the SSL encryption.

The upcoming sections describe how to handle these features. The description begins with an overview.

4.1

Overview

The following overview shows the sections that are in this chapter:

User's Guide SSL Scanner	
<i>Introduction</i>	
<i>Home</i>	
<i>Common</i>	
SSL Scanner	Overview – <i>this section</i>
<i>Policy Settings</i>	Certificate Verification, see 4.2
	Scan Encrypted Traffic, see 4.3
	Certificate List, see 4.4
	Trusted Certificate Authorities, see 4.5
<i>Policy-Independent Settings</i>	Global Certificate List, see 4.6
	Global Trusted Certificate Authorities, see 4.7
	Incident Manager, see 4.8

4.2

Certificate Verification

The *Certificate Verification* options are invoked by clicking on the corresponding button under *SSL Scanner*:

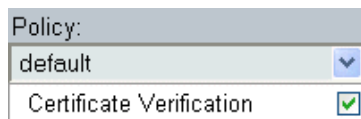
Certificate Verification	<input checked="" type="checkbox"/>
--------------------------	-------------------------------------

If you want to enable any of these options, make sure the checkbox on this button is also marked. The checkbox is marked by default.

After modifying the setting of this checkbox, click on *Apply Changes* to make the modification effective.

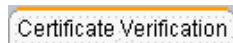
These are policy-dependent options, i. e. they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled *Policy*, which is located above the *Certificate Verification* button:



Policy:
default
Certificate Verification

The options are arranged under the following tab:



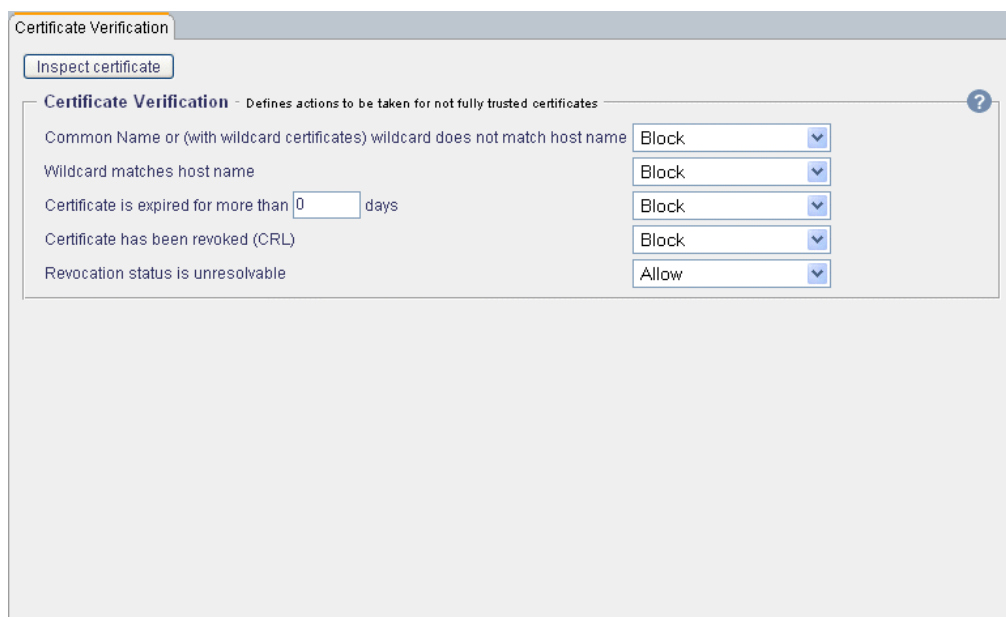
Certificate Verification

They are described in the upcoming section:

- *Certificate Verification*, see [4.2.1](#)

4.2.1 Certificate Verification

The *Certificate Verification* tab looks like this:



Certificate Verification

Inspect certificate

Certificate Verification - Defines actions to be taken for not fully trusted certificates

Common Name or (with wildcard certificates) wildcard does not match host name	Block
Wildcard matches host name	Block
Certificate is expired for more than 0 days	Block
Certificate has been revoked (CRL)	Block
Revocation status is unresolvable	Allow

At the top of this tab, there is the following button:



Inspect certificate

Click on this button to inspect the certificate of a particular host. This will open a window, where you can specify the host and retrieve the certificate.

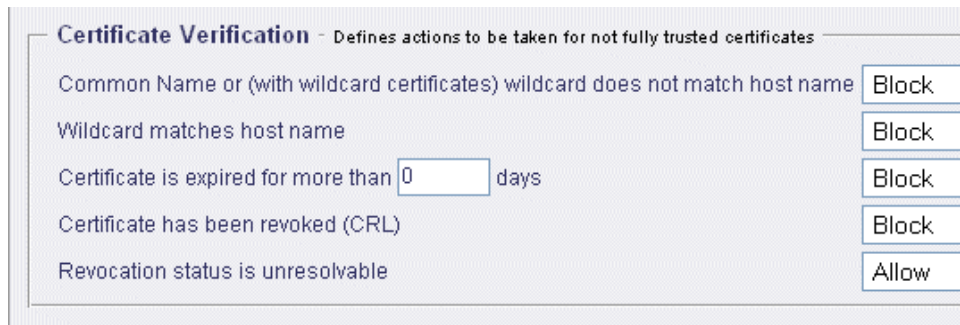
Furthermore, there is this section on the tab:

- *Certificate Verification*

It is described in the following.

Certificate Verification

The *Certificate Verification* section looks like this:



The screenshot shows a configuration window titled "Certificate Verification" with the subtitle "Defines actions to be taken for not fully trusted certificates". It contains five rows of settings, each with a text label and a dropdown menu:

Condition	Action
Common Name or (with wildcard certificates) wildcard does not match host name	Block
Wildcard matches host name	Block
Certificate is expired for more than <input type="text" value="0"/> days	Block
Certificate has been revoked (CRL)	Block
Revocation status is unresolvable	Allow

Using this section, you can configure actions for particular verification tests.

After specifying the appropriate settings, click on *Apply Changes* to make them effective.

Verification tests can be configured and performed according to the following criteria:

- *Common Name or (with wildcard certificates) wildcard does not match host name*

Compares the Common Name used in a certificate for a host to the host name as given by the corresponding URL. In some certificates the Common Name is represented by a wildcard with shell expressions being used (wildcard certificates).

If no match can be established between a regular Common Name and the host name, the verification process looks for a wildcard and compares it to the host name. If this does not lead to a match either, the configured action is executed.

One of the major features of trying to achieve security through trusted certificates is to guarantee the identity of a remote server. Therefore, it is imperative that the Common Name of a certificate is identical to the URL of the corresponding Web server.

If you allow a connection nevertheless, there is no guarantee that spoofing (a Web site impersonates the Web site you actually wanted to visit) has not occurred.

If the Common Name in a certificate is, e. g. [abcde.com](#), but the Web server's URL is in fact [www.abcde.com](#), no match is achieved.

- *Wildcard matches host name*

Compares the wildcard used in a certificate to represent a Common Name to the host name. So, e. g. the wildcard expression [*.ccc.de](#) matches [www.ccc.de](#).

If a match is achieved, the configured action will be executed.

- *Certificate is expired for more than ... days*

Checks if a certificate has expired. If more than the number of days configured here have elapsed since expiration of the certificate, the configured action will be executed. A grace period may allow the use of the certificate even after it has expired.

Enter the desired number of days in the input field provided with this option.

- *Certificate is revoked*

Checks if a certificate has been revoked. For this purpose, the Certificate Revocation List (CRL) is used. If the certificate has been revoked, the configured action will be executed.

- *Revocation status is unresolvable*

The reason why the revocation status is unresolvable could be that the corresponding certificate authority or the path leading to the Certificate Revocation List (CRL) is not known.

4.3

Scan Encrypted Traffic

The *Scan Encrypted Traffic* options are invoked by clicking on the corresponding button under *SSL Scanner*:

Scan Encrypted Traffic	<input checked="" type="checkbox"/>
------------------------	-------------------------------------

If you want to enable any of these options, make sure the checkbox on this button is also marked. The checkbox is marked by default.

After modifying the setting of this checkbox, click on *Apply Changes* to make the modification effective.

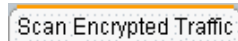
These are policy-dependent options, i. e. they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled *Policy*, which is located above the *Certificate Verification* button:



The screenshot shows a 'Policy:' label above a dropdown menu with 'default' selected. Below the dropdown is a 'Certificate Verification' button with a green checkmark icon.

The options are arranged under the following tab:



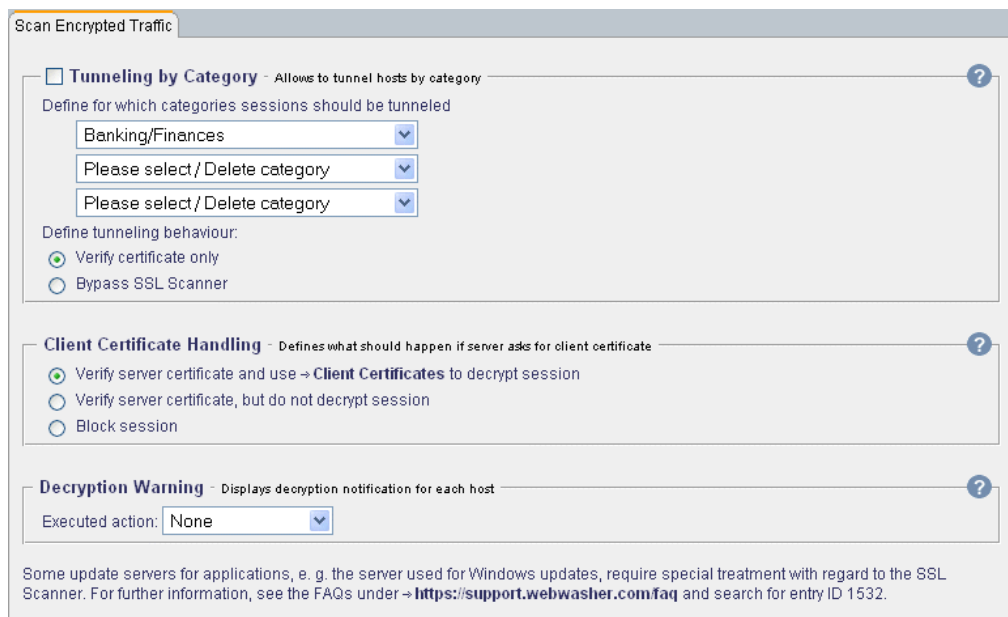
The screenshot shows a single tab labeled 'Scan Encrypted Traffic'.

They are described in the upcoming section:

- *Scan Encrypted Traffic*, see [4.3.1](#)

4.3.1 Scan Encrypted Traffic

The *Scan Encrypted Traffic* tab looks like this:



The screenshot shows the 'Scan Encrypted Traffic' configuration tab with three main sections:

- Tunneling by Category** - Allows to tunnel hosts by category. Includes a checkbox, a description, and three dropdown menus for category selection. The first dropdown is set to 'Banking/Finances'. Below are two radio buttons: 'Verify certificate only' (selected) and 'Bypass SSL Scanner'.
- Client Certificate Handling** - Defines what should happen if server asks for client certificate. Includes three radio buttons: 'Verify server certificate and use → Client Certificates to decrypt session' (selected), 'Verify server certificate, but do not decrypt session', and 'Block session'.
- Decryption Warning** - Displays decryption notification for each host. Includes a dropdown menu for 'Executed action' set to 'None'.

At the bottom, there is a note: 'Some update servers for applications, e. g. the server used for Windows updates, require special treatment with regard to the SSL Scanner. For further information, see the FAQs under → <https://support.webwasher.com/faq> and search for entry ID 1532.'

There are three sections on this tab:

- *Tunneling by Category*
- *Client Certificate Handling*
- *Decryption Warning*

They are described in the upcoming sections.

Tunneling by Category

The *Tunneling by Category* section looks like this:

Using this section, you can configure tunneling for particular URL filtering categories. You can configure up to three categories for tunneling. These may pre-defined or user-defined categories.

If you want to use additional categories, you need to enter them in the *<policy>.ini* configuration file, which is located in the *conf* folder of the Webwasher program files.

This tunneling option is not enabled by default. If you want to enable it, mark the checkbox next to the section heading.

After specifying the appropriate information, click on *Apply Changes* to make your settings effective.

Use the items in the following areas to configure tunneling by category:

- *Define for which categories sessions should be tunneled*

Select up to three categories from the drop-down lists provided here. Categories may be selected from pre-defined or user-defined categories.

To delete a category, click on the *Please select / Delete category* list item in the corresponding drop-down list.

- *Define tunneling behavior*

To determine what tunneling should mean for the selected categories, enable one of these options:

- *Verify certificate only*

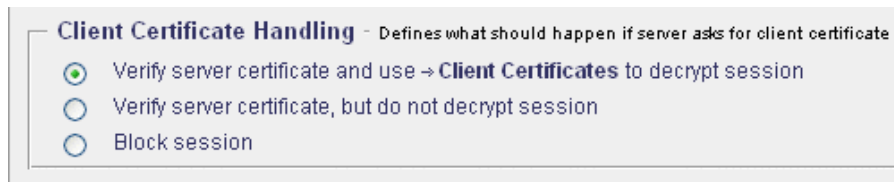
The certificate belonging to the requested URL is checked by a verification procedure, but no other activities are performed by the SSL Scanner.

— *Bypass SSL Scanner*

The SSL Scanner is bypassed completely, i. e. no activities whatsoever are performed.

Client Certificate Handling

The *Client Certificate Handling* section looks like this:



Using this section, you can configure what should happen if the server that is requested by a client asks for a client certificate.

Using this section, you can configure tunneling for particular URL filtering categories. You can configure up to three categories for tunneling. These may pre-defined or user-defined categories.

If you want to use additional categories, you need to enter them in the *global.ini* configuration file, which is located in the *conf* folder of the Web-washer program files.

This tunneling option is not enabled by default. If you want to enable it, mark the checkbox next to the section heading.

After specifying the appropriate information, click on *Apply Changes* to make your settings effective.

Use the following radio buttons to configure the handling of client certificates:

- *Verify server certificate and use client certificates to decrypt session*

Enable this option to have both the server and the client certificate, i. e. the certificate the client was requested to submit by the server, checked by the verification process.

The certificate list is searched for the client certificate in order to authenticate the client. If the search has been successful, the session will be allowed and the communication decrypted. If no appropriate client certificate is found, the request will be denied.

Clicking on the *Client Certificates* link provided with this option, takes you to the *Client Certificate* tab, where you can add more certificates to this list.

- *Verify server certificate, but do not decrypt session*

Enable this option, to have the server certificate checked by the verification process.

If this is passed successfully, the corresponding session is tunneled and allowed.

- *Block Session*

Enable this option to forbid access to the server.

Decryption Warning

The *Decryption Warning* section looks like this:



Using this section, you can configure a decryption warning for HTTPS traffic. It is inserted whenever a request to a domain (without a path) is made that involves this kind of traffic.

The warning includes a button to click on in case you want to proceed and view the requested page.

After specifying the appropriate information, click on *Apply Changes* to make this setting effective.

Use the following drop-down list to configure a decryption warning:

- *Executed action*

Select *Warning Decryption* to configure the warning. Select *None* to have no warning.

4.4

Certificate List

The *Certificate List* options are invoked by clicking on the corresponding button under *SSL Scanner*:



If you want to enable any of these options, mark the checkbox that is on this button.

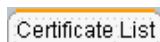
Then click on *Apply Changes* to make this setting effective.

These are policy-dependent options, i. e. they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled *Policy*, which is located above the *Certificate Verification* button:



The options are arranged under the following tab:

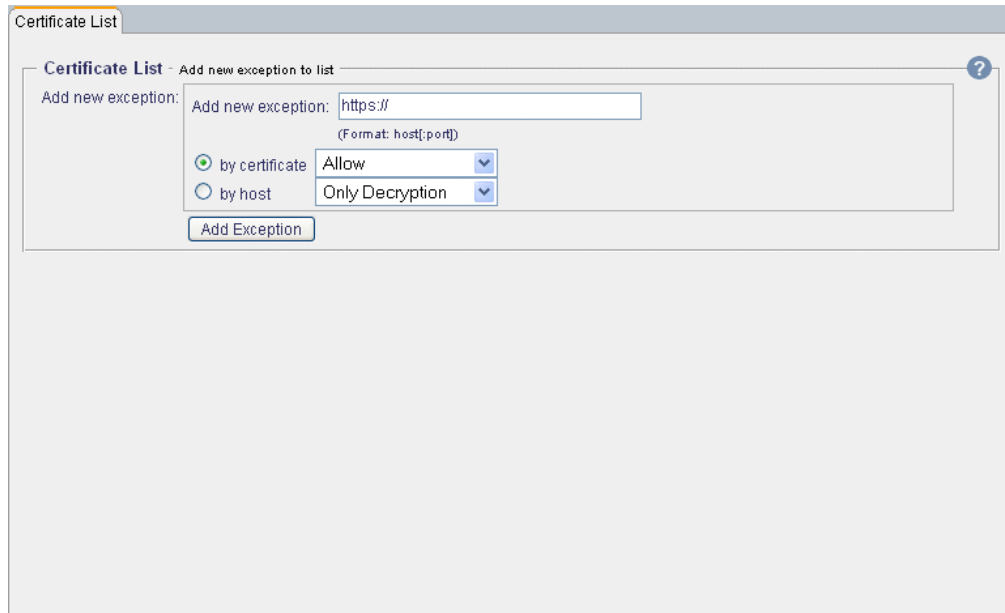


They are described in the upcoming section:

- *Certificate List*, see [4.4.1](#)

4.4.1 Certificate List

The *Certificate List* tab looks like this:



The screenshot shows the 'Certificate List' tab in the SSL Scanner application. The tab title is 'Certificate List' and the subtitle is 'Add new exception to list'. There is a help icon (?) in the top right corner. The main content area is titled 'Add new exception:' and contains a text input field with the value 'https://'. Below the input field is the text '(Format: host[:port])'. There are two radio buttons: 'by certificate' (selected) and 'by host'. To the right of the 'by certificate' radio button is a dropdown menu with 'Allow' selected. To the right of the 'by host' radio button is a dropdown menu with 'Only Decryption' selected. At the bottom of the form is an 'Add Exception' button.

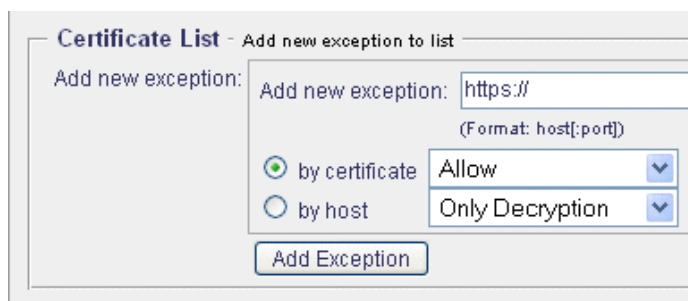
There is one section on this tab:

- *Certificate List*

It is described in the following.

Certificate List

The *Certificate List* section looks like this:



The screenshot shows the 'Certificate List' section in the SSL Scanner application. The section title is 'Certificate List' and the subtitle is 'Add new exception to list'. There is a help icon (?) in the top right corner. The main content area is titled 'Add new exception:' and contains a text input field with the value 'https://'. Below the input field is the text '(Format: host[:port])'. There are two radio buttons: 'by certificate' (selected) and 'by host'. To the right of the 'by certificate' radio button is a dropdown menu with 'Allow' selected. To the right of the 'by host' radio button is a dropdown menu with 'Only Decryption' selected. At the bottom of the form is an 'Add Exception' button.

Using this section, you can add new exceptions to the list of certificates. You can also configure actions for an exception relating to the certificate or host in question.

To add an exception to the list, use the area labeled:

- *Add new exception*

In the input field provided here, enter the exception you want to add to the certificate list.

https:// has been entered in this field as default information at the beginning of an exception name. The input format for its remaining parts is:

host [:port]

Furthermore, configure the following methods for a new exception:

- *by certificate*

Enabling the *by certificate* method means that the certificate issued for the host you are adding as an exception is checked by the verification process.

After enabling this method, select an action from the drop-down list provided here.

For the meaning of these actions, see the following table:

	<i>by certificate</i>	<i>by host</i>
<i>Allow</i>	The exception is allowed.	<i>not available</i>
<i>Block</i>	The exception is blocked.	The exception is blocked.
<i>Tunnel</i>	The activities of the SSL Scanner are bypassed and no verification process is executed.	The activities of the SSL Scanner are bypassed and no verification process is executed.
<i>Warn Incident</i>	The exception is allowed, but a warning is displayed.	<i>not available</i>
<i>Only Cert Checking</i>	<i>not available</i>	The content provided by the host you are adding as an exception is not decrypted, and the exception is allowed. <i>Note:</i> In this case, the certificate will be checked.
<i>Only Decryption</i>	<i>not available</i>	The content provided by the host you are adding as an exception is decrypted, and the exception is allowed.

— *by host*

Enabling the *by host* method means that the host is checked without a certificate being included in the verification process. If the latter method is chosen, shell expressions, e. g. **.webwasher.com*, may be used to specify an exception.

After enabling this method, select an action from the drop-down list provided here.

For the meaning of these actions, see the description of the *by certificate* method above.

— *Add exception*

After specifying the appropriate settings, click on this button to add an exception to the list.

Enabling the *by host* method means that the host is checked without a certificate being included in the verification process. If the latter method is chosen, shell expressions, e. g. **.webwasher.com*, may be used to specify an exception.

After enabling this method, select an action from the drop-down list provided here.

For the meaning of these actions, see the description of the *by certificate* method above.

A message will then be displayed, stating if the exception has been added successfully and providing information on the result of the verification process.

If the by certificate method has been configured, you are informed whether the certificate in question was issued by a trusted or not-trusted certification authority (CA) from the corresponding list.

If the CA could not be found on this list, the certificate is implicitly forbidden.

If the inspection of a certificate results in an error or open issue, the depth of the certificate is also stated in the corresponding error message. By depth is meant the position the certificate takes within the certificate chain.

So, e. g. *depth = 0* means the certificate has been issued immediately for the software in question, as is the case with self-signed certificates, *depth = 1* is for a certificate issued to certify a *depth 0* certificate and so on.

The newly added exception will be shown in a list displayed below.

To display only a particular number of list entries at a time, type this number in the input field labeled *Number of entries per page* and enter it using the *Enter* key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

You can also edit this list, by specifying the appropriate settings for a given entry. After doing this, click on *Apply Changes* to make these settings effective.

Use the following items to perform other activities relating to the list:

- *Filter*

Type a filter expression in this input field and enter it using the *Enter* key of your keyboard. The list will then display only entries matching the filter.

- *Delete Selected*

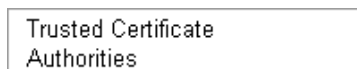
Select the entry you wish to delete by marking the *Select* checkbox next to it and click on this button. You can delete more than one entry in one go.

To delete all entries, mark the *Select all* checkbox and click on this button.

4.5

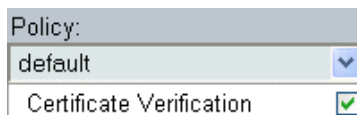
Trusted Certificate Authorities

The *Trusted Certificate Authorities* options are invoked by clicking on the corresponding button under *SSL Scanner*:



These are policy-dependent options, i. e. they are configured for a particular policy. When you are configuring these options, you need to specify this policy.

To do this, select a policy from the drop-down list labeled *Policy*, which is located above the *Certificate Verification* button:



The options are arranged under the following tab:



They are described in the upcoming section:

- *Trusted Certificate Authorities*, see [4.5.1](#)

4.5.1 Trusted Certificate Authorities

The *Trusted Certificate Authorities* tab looks like this:

The screenshot shows the 'Trusted Certificate Authorities' tab. At the top, there is a link to 'Known Certificate Authorities' to add or delete global Certificate Authorities. Below this, there are two main sections:

Certificate Authorities - Actions for CAs

- First known CA is trusted: Allow
- First known CA is untrusted: Block
- Only unknown CAs found: Block

Trusted Certificate Authorities - Add a CA to your list

Select CA: ABA,ECOM,INC.
(Note: If the drop down box is empty, all known CAs are already in this list)

Trust Do not trust Add to all policies

Found 2 entries with "*" Number of entries per page: 15

Select	Certificate Authority	Trusted
<input type="checkbox"/>	Belgacom	<input checked="" type="checkbox"/> Trusted
<input type="checkbox"/>	C&W HKT SecureNet CA Class A	<input type="checkbox"/> Trusted

Select All

At the top of this tab, there is the *Known Certificate Authorities* link.

A click on this link will take you to the tab with the same name, where you can add Certificate Authorities to the list or delete them.

Furthermore, there are two sections on this tab:

- *Certificate Authorities*
- *Trusted Certificate Authorities*

They are described in the following.

Certificate Authorities

The *Certificate Authorities* section looks like this:

The screenshot shows the 'Certificate Authorities - Actions for CAs' section. It contains three dropdown menus:

- First known CA is trusted: Allow
- First known CA is untrusted: Block
- Only unknown CAs found: Block

Using this section, you can configure actions for content with certificates issued by known Certificate Authorities (CAs) that are either trusted or untrusted, as well as for unknown Certificate Authorities.

A vendor, having signed content by issuing a certificate, may request a CA to issue a certificate to sign this vendor certificate. This CA may itself have been signed by another CA, issuing certificates on a higher level. Together, these certificates form a certificate chain, which is inspected in a verification process. The CA that signed a certificate located on a lower level of the certificate chain is also called the root CA.

The verification process begins by checking the CA that immediately signed the vendor certificate. It may be known, i. e., be included in the list of known CAs. If the CA is unknown, the verification process checks the CA on the next level and goes on to do so, until a known CA is found, or all CAs in the certificate chain have proven to be unknown. Usually, there are no more than three levels to a certificate chain.

The first known CA to be found in the verification process is then checked as to whether it is trusted or untrusted. To be trusted, a CA must be included in the list of trusted CAs.

The list of trusted CAs is configured in the [Trusted Certificate Authorities](#) section, which is also provided on this tab.

To edit the list of known CAs, use the [Known Certificate Authorities](#) link, which is located at the top of this tab, to go to the tab provided for this purpose.

When configuring actions for trusted CAs, remember that you have to select actions that include a [Log Incident](#) part, e. g. [Block & Log Incident](#), if you want to have incidents related to these CAs listed by the incident manager.

After specifying the appropriate settings here, click on [Apply Changes](#) to make them effective.

Use the drop-down lists provided here to configure actions for the following situations:

- [First known CA is trusted](#)

Select an action here that should be taken if the first known CA is trusted.

- [First known CA is untrusted](#)

Select an action here that should be taken if the first known CA is untrusted.

- [Only unknow CAs found](#)

Select an action here that should be taken if only unknown CAs have been found.

Trusted Certificate Authorities

The *Trusted Certificate Authorities* section looks like this:

Trusted Certificate Authorities - Add a CA to your list

Select CA:
(Note: If the drop down box is empty, all known CAs are already in this list)

Add to all policies

Found 2 entries with **

Select	Certificate Authority
<input type="checkbox"/>	Belgacom
<input type="checkbox"/>	C&W HKT SecureNet CA Class A

Select All

This section provides the list of Trusted Certificate Authorities (CAs). Also provided is a list of known CAs, from which you can select CAs to include them in the list of trusted CAs. When including a CA in this list, you can configure it as trusted or not trusted.

If a CA has been included in the list of trusted CAs as not trusted, certificates issued by it will be explicitly forbidden, i. e. will also not be trusted. This is indicated in status messages referring to a certificate.

If a CA is not included in the list at all, certificates issued by it may be implicitly forbidden, which is also indicated in status messages.

Note that besides this list, which is configured only for a particular policy, there is also the list of Global Trusted Certificate Authorities. If a CA does not appear in the list of trusted CAs configured here, the settings configured for the global list will apply.

To select a CA from the list of known CAs and add it to the list of trusted CAs, use the area labeled:

- *Select CA*

Select the CA you want to add to the list of trusted CAs from the drop-down list provided here.

If this list is empty, it means that all known CAs have been included in the list of trusted CAs, either as trusted or not trusted.

The addition of a CA here will be valid only under the policy you are currently configuring.

To make the addition valid for all policies, mark the checkbox labeled *Add to all policies* before proceeding any further.

Then click on either of these two buttons, according to whether you want to add the CA as trusted or not trusted:

— *Trust*

Click on this button to add a CA to the list as trusted.

— *Do not trust*

Click on this button to add a CA to the list as not trusted.

The list of trusted CAs is displayed at the bottom of this section.

To display only a particular number of list entries at a time, type this number in the input field labeled *Number of entries per page* and enter it using the *Enter* key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To sort the list in ascending or descending order, click on the symbol next to the *Certificate Authority* column heading.

To change the status of CA from trusted to not trusted or the other way round, mark or clear the *Trusted* checkbox in the same line.

Then click on *Apply Changes* to make this setting effective. You can edit more than one list entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- *Filter*

Type a filter expression in this input field and enter it using the *Enter* key of your keyboard. The list will then display only entries matching the filter.

- *Delete Selected*

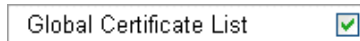
Select the list entry you wish to delete by marking the *Select* checkbox next to it and click on this button. You can delete more than one entry in one go.

To delete all entries, mark the *Select all* checkbox and click on this button.

4.6

Global Certificate List

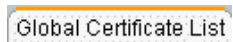
The *Global Certificate List* options are invoked by clicking on the corresponding button under *SSL Scanner*:



If you want to enable any of these options, make sure the checkbox on this button is marked. The checkbox is marked by default.

After modifying the setting of this checkbox, click on *Apply Changes* to make the modification effective.

The options are arranged under the following tab:



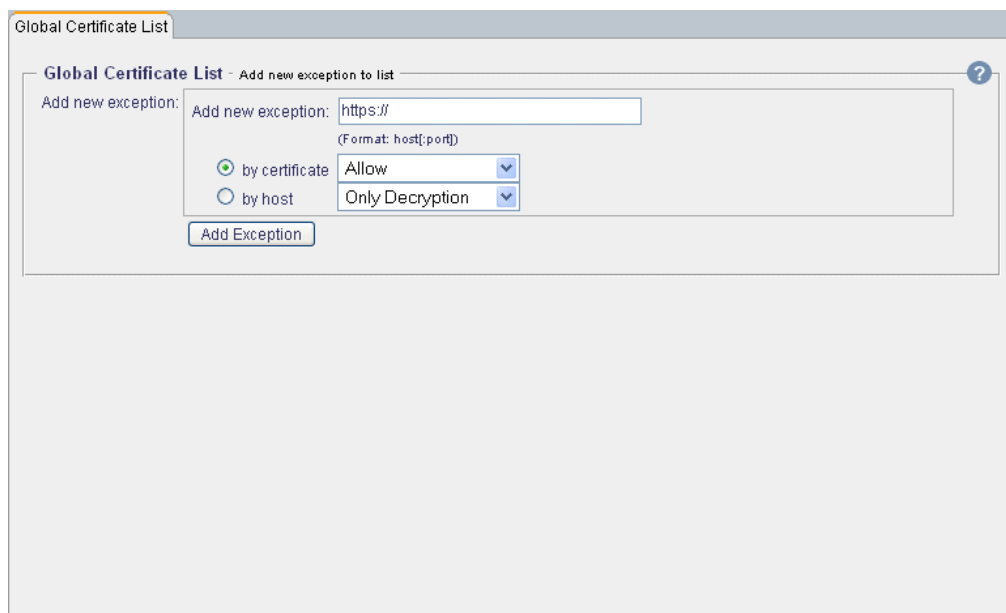
They are described in the upcoming section:

- *Global Certificate List*, see [4.6.1](#)

4.6.1

Global Certificate List

The *Global Certificate List* tab looks like this:



There is one section on this tab:

- *Global Certificate List*

It is described in the following.

Global Certificate List

The *Global Certificate List* section looks like this:



Using this section, you can add new exceptions to the global list of certificates, i. e. to the list that is valid for all policies configured under Webwasher.

You can also configure actions for an exception relating to the certificate or host in question.

To add an exception to the list, use the area labeled:

- *Add new exception*

In the input field provided here, enter the exception you want to add to the global certificate list.

https:// has been entered in this field as default information at the beginning of an exception name. The input format for its remaining parts is:

host [:port]

Furthermore, configure the following methods for a new exception:

- *by certificate*

Enabling the *by certificate* method means that the certificate issued for the host you are adding as an exception is checked by the verification process.

After enabling this method, select an action from the drop-down list provided here.

For the meaning of these actions, see the following table:

	<i>by certificate</i>	<i>by host</i>
<i>Allow</i>	The exception is allowed.	<i>not available</i>
<i>Block</i>	The exception is blocked.	The exception is blocked.
<i>Tunnel</i>	The activities of the SSL Scanner are bypassed and no verification process is executed.	The activities of the SSL Scanner are bypassed and no verification process is executed.
<i>Warn Incident</i>	The exception is allowed, but a warning is displayed.	<i>not available</i>
<i>Only Cert Checking</i>	<i>not available</i>	The content provided by the host you are adding as an exception is not decrypted, and the exception is allowed. <i>Note:</i> In this case, the certificate will be checked.
<i>Only Decryption</i>	<i>not available</i>	The content provided by the host you are adding as an exception is decrypted, and the exception is allowed.

— *by host*

Enabling the *by host* method means that the host is checked without a certificate being included in the verification process. If the latter method is chosen, shell expressions, e. g. **.webwasher.com*, may be used to specify an exception.

After enabling this method, select an action from the drop-down list provided here.

For the meaning of these actions, see the description of the *by certificate* method above.

— *Add exception*

After specifying the appropriate settings, click on this button to add an exception to the list.

Enabling the *by host* method means that the host is checked without a certificate being included in the verification process. If the latter method is chosen, shell expressions, e. g. **.webwasher.com*, may be used to specify an exception.

After enabling this method, select an action from the drop-down list provided here.

For the meaning of these actions, see the description of the *by certificate* method above.

A message will then be displayed, stating if the exception has been added successfully and providing information on the result of the verification process.

If the by certificate method has been configured, you are informed whether the certificate in question was issued by a trusted or not-trusted certification authority (CA) from the corresponding list.

If the CA could not be found on this list, the certificate is implicitly forbidden.

If the inspection of a certificate results in an error or open issue, the depth of the certificate is also stated in the corresponding error message. By depth is meant the position the certificate takes within the certificate chain.

So, e. g. *depth = 0* means the certificate has been issued immediately for the software in question, as is the case with self-signed certificates, *depth = 1* is for a certificate issued to certify a *depth 0* certificate and so on.

The newly added exception will be shown in a list displayed below.

To display only a particular number of list entries at a time, type this number in the input field labeled *Number of entries per page* and enter it using the *Enter* key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

You can also edit this list, by specifying the appropriate settings for a given entry. After doing this, click on *Apply Changes* to make these settings effective.

Use the following items to perform other activities relating to the list:

- *Filter*

Type a filter expression in this input field and enter it using the *Enter* key of your keyboard. The list will then display only entries matching the filter.

- *Delete Selected*

Select the entry you wish to delete by marking the *Select* checkbox next to it and click on this button. You can delete more than one entry in one go.

To delete all entries, mark the *Select all* checkbox and click on this button.

4.7

Global Trusted Certificate Authorities

The *Global Trusted Certificate Authorities* options are invoked by clicking on the corresponding button under *SSL Scanner*:

Global Trusted Certificate Authorities

The options are arranged under the following tab:

Global Trusted Certificate Authorities

They are described in the upcoming section:

- *Global Trusted Certificate Authorities*, see [4.7.1](#)

4.7.1

Global Trusted Certificate Authorities

The *Global Trusted Certificate Authorities* tab looks like this:

The screenshot shows the 'Global Trusted Certificate Authorities' tab. At the top, it says 'Trusted Certificate Authorities - Add a CA to your list'. Below this is a 'Select CA:' dropdown menu with 'ABA.ECOM, INC.' selected. A note below the dropdown reads: '(Note: If the drop down box is empty, all known CAs are already in this list)'. There is a 'Trust' button below the dropdown. Below the 'Trust' button, it says 'Found no entry with **'. There is a 'Select' dropdown menu with 'Certificate Authority' selected. Below the 'Select' dropdown is a 'Filter:' text input field. At the bottom, there are two buttons: 'Select All' and 'Delete Selected'.

There is one section on this tab:

- *Trusted Certificate Authorities*

It is described in the following.

Trusted Certificate Authorities

The *Trusted Certificate Authorities* section looks like this:

The screenshot shows a web interface for managing Trusted Certificate Authorities. At the top, it says "Trusted Certificate Authorities - Add a CA to your list". Below this is a "Select CA:" dropdown menu with "ABA, ECOM, INC." selected. A note below the dropdown reads: "(Note: If the drop down box is empty, all known CAs are already in this list)". Below the note is a "Trust" button. Further down, it says "Found no entry with *". Below that is a "Select" dropdown menu with "Certificate Authority" selected. To the right of the dropdown is a "Filter:" input field. At the bottom, there are two buttons: "Select All" and "Delete Selected".

This section provides the global list of Trusted Certificate Authorities (CAs), i. e. the list that is valid for all policies configured under Webwasher.

If a CA is also in a policy-dependent list, the settings configured for this list will prevail.

Also provided is a list of known CAs, from which you can select CAs to include them in the list of trusted CAs.

To select a CA from the list of known CAs and add it to the list of trusted CAs, use the area labeled:

- *Select CA*

Select the CA you want to add to the list of trusted CAs from the drop-down list provided here.

If this list is empty, it means that all known CAs have been included in the list of trusted CAs.

To add the CA you select, use the following button:

— *Trust*

Click on this button to add a CA to the list as trusted.

The list of trusted CAs is displayed at the bottom of this section.

To display only a particular number of list entries at a time, type this number in the input field labeled *Number of entries per page* and enter it using the *Enter* key of your keyboard.

If the number of entries is higher than this number, the remaining entries are shown on successive pages. A page indicator is then displayed, where you can select a particular page by clicking on the appropriate arrow symbols.

To sort the list in ascending or descending order, click on the symbol next to the *Certificate Authority* column heading.

To change the status of CA from trusted to not trusted or the other way round, mark or clear the *Trusted* checkbox in the same line.

Then click on *Apply Changes* to make this setting effective. You can edit more than one list entry and make the changes effective in one go.

Use the following items to perform other activities relating to the list:

- *Filter*

Type a filter expression in this input field and enter it using the *Enter* key of your keyboard. The list will then display only entries matching the filter.

- *Delete Selected*

Select the list entry you wish to delete by marking the *Select* checkbox next to it and click on this button. You can delete more than one entry in one go.

To delete all entries, mark the *Select all* checkbox and click on this button.

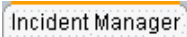
4.8

Incident Manager

The *Incident Manager* options are invoked by clicking on the corresponding button under *SSL Scanner*:



The options are arranged under the following tab:

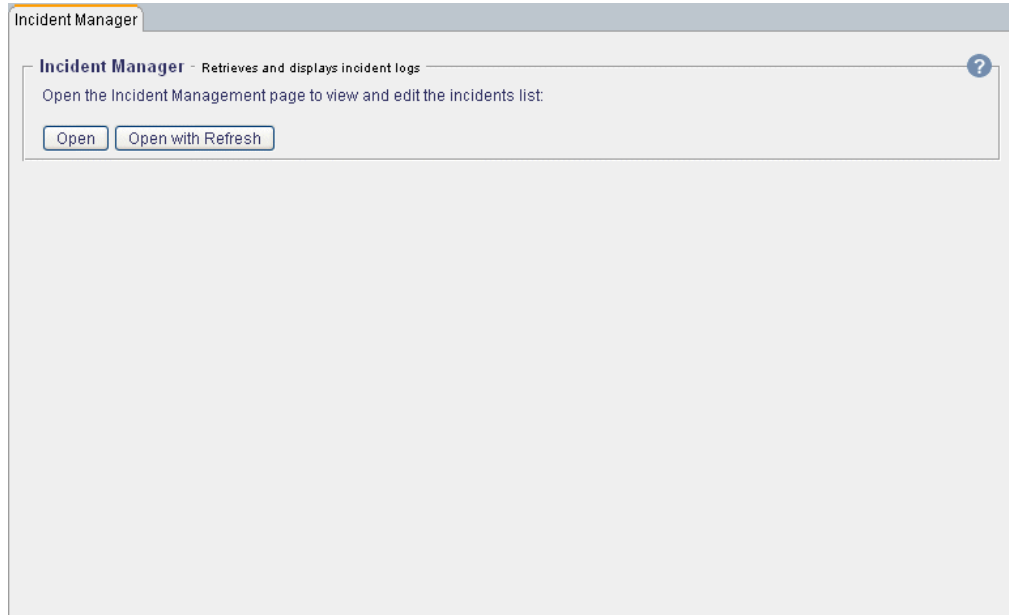


They are described in the upcoming section:

- *Incident Manager*, see [4.8.1](#)

4.8.1 Incident Manager

The *Incident Manager* tab looks like this:



There is one section on this tab:

- *Incident Manager*

It is described in the following.

Incident Manager

The *Incident Manager* section looks like this:



Using this section, you can inspect and manage incidents relating to SSL-encrypted communication.

The Incident Manager enables you to retrieve *incident.dat* files from Webwasher instances. It synchronizes and displays them, adding hosts or certificates to the policy-dependent or independent (global) certificate list.

Note that an *incident.dat* file will only be written if you have configured an *Allow & Log Incident* or *Block & Log Incident* action or a user defined action that leads to writing a log file.

You can view and edit the incidents list on the *Incident Management* page. It is opened with or without a refresh by clicking on one of the following buttons:

or:

For a description of this page, see the next section.

Incident Management

Using the *Incident Management* page, you can inspect SSL incidents and add them either to the policy-dependent or independent (global) certificate list.

On this page, a table is provided listing all incidents that occurred after the last refresh of this list was performed. All of them have not yet been processed.

<input type="checkbox"/> Select All on Page <input type="button" value="Delete"/> <input type="button" value="Add"/>					
Host▼					
C	E	S	R	Policy	Action
Filter: <input type="text"/> <input type="button" value="Clear Filter"/> Found no entry out of 0 with ""					
<input type="checkbox"/> Select All on Page <input type="button" value="Delete"/> <input type="button" value="Add"/>					

To perform a refresh, click on the *Refresh Incident List* button, which is located above the left side of the table:

This will process the stored incidents and add them to the list.

If Webwasher is running in a cluster, a refresh will lead to a synchronization with the subscribed sites. Depending on the sites load, the refresh may take a moment.

The list will be cross-checked with the policy-dependent and independent certificate lists to avoid multiple entries.

A list entry consists of the following fields:

- *Host* - URL that caused the incident.

Incidents can be added to the certificate lists either *by host* or *by certificate*, as is shown in the fields used for configuring the policy-dependent and independent certificate lists. If *by host* was selected, the input shown here under *Host* becomes available.

A wildcard may be used to include a range of URLs, e. g.
**.webwasher.com*.

- *C (short for Common Name)* - If an incident was caused by a Common Name mismatch, it is indicated here by a red lamp symbol. Otherwise there will be a green lamp symbol.
- *E (short for Expired)* - If a certificate has expired, this incident is indicated here by a red lamp symbol.
- *S (short for Self-signed)* - If an incident was caused by a self-signed certificate, it is indicated here by a red lamp symbol.
- *R (short for Root Certificate Authority)* - If an incident was caused by a failure during validation of the root certificate authority, it is indicated here.
- *Policy* - Policy belonging to the certificate list this incident is going to be added to.
- *Action* - Action configured for the policy and host/certificate that will apply when the incident is added to a certificate list.

The list is sortable by *Host* and the *C(ommon Name)*, *E(xpired)*, *S(elf-signed)* and *R(oot Certificate Authority)* failure attributes.

Note: An incident that occurred for two or more different reasons, cannot be added *by certificate*.

Whenever a certificate is added this way, errors that were caused by the certificate are ignored. Different reasons may occur, however, when a certificate is inspected with regard to different policies.

If errors cannot be determined unambiguously, as is the case when there are two or more reasons for an incident, the *by certificate* method cannot be applied. Incidents can then only be added *by host*.

You can select several incidents from the list and add or delete them in one go by clicking on the *Add* or the *Delete* button. If you wish to process an entry separately, use the *Add* and *Delete* buttons in the same line.

If an incident was deleted from the list, it will not be ignored in the future, but be generated again should it occur.