
IceWarp Server

AntiSpam QuickStart Guide

Version 9.3



Contents

IceWarp Server AntiSpam Quick Start 3

Introduction.....	3
How it works.....	3
AntiSpam Templates	4
General.....	5
Other	5
Logging	6
Outgoing Messages.....	6
Other.....	6
Advanced	6
Action	7
General	7
Refusal	7
Spam	8
Reports	8
Quarantine	9
General	9
Options.....	9
Challenge Response.....	10
SpamAssassin	10
General	10
Reporting	11
RBL.....	11

Anti-Spam Live 12

Bayesian Filters 12

Black & White List..... 13

 Blacklist..... 13

 General..... 13

 Keywords 13

 Whitelist 13

 General..... 14

 Advanced 14

 Keywords 14

Greylisting..... 15

Learning Rules 15

Miscellaneous..... 16

 Content 16

 Charset 16

 Sender 17

CHAPTER 1

IceWarp Server AntiSpam Quick Start

In This Chapter

Introduction	3
How it works	3
AntiSpam Templates	4
General	5
Action	7
Quarantine	9
SpamAssassin	10
Anti-Spam Live	12
Bayesian Filters	12
Black & White List	13
Greylisting	15
Learning Rules	15
Miscellaneous	16

Introduction

This quick guide will get your IceWarp Server's AntiSpam up and running with a basic set of recommended settings, allowing you to start protecting your users from spam immediately.

All settings can be found in the IceWarp Server GUI - subnodes of the AntiSpam node, and are discussed in order.

For more detailed information on the AntiSpam settings you should read the AntiSpam Reference manual, or press F1 whilst in the GUI for context-sensitive help.

How it works

In the following chapters you will be provided with necessary information about AntiSpam filters. All messages are processed by multiple AntiSpam filters and if a filter is matched then a spam score is increased. Dependent on the spam score value at the end of AntiSpam processing the following actions can be taken:

Quarantine the message – stores the messages in a quarantine queue and allows you and your users to decide which are spam and which are not.

Classify the message as a spam – marks the message with the specific spam score allowing IceWarp Server to process it according to its settings.

Refuse the message – If the spam score is so high that it is definitely spam, the message is automatically rejected/deleted.

Note - that some messages may not be processed by AntiSpam if they match certain bypass criteria, which are discussed later.

AntiSpam Templates

The AntiSpam default settings are based on the experiences of our customers, who process millions of messages per day.

The settings are well-balanced, but you can make them more or less restrictive by selecting predefined templates. These templates can be found at the bottom of every AntiSpam screen, and you can select from High, Medium and Low levels of protection:

Low – this is the least resource-hungry template but will not catch as much spam as the other settings.

The following features are not used with the Low template enabled: Greylisting, Quarantine, SpamAssassin SPF, Razor2 and DomainKeys.

Medium – This is the recommended option. It uses more server resources for the extra processing but with a much better chance of correctly identifying Spam.

Greylisting, Quarantine and SPF technology are enabled, Spam Classification scores lowered.

High - The most resource-hungry template, with the best chance of correctly identifying Spam but with an increased chance of false positives. All available technologies are used (except for AntiSpam Live, which requires a standalone license and is therefore not included in any template).

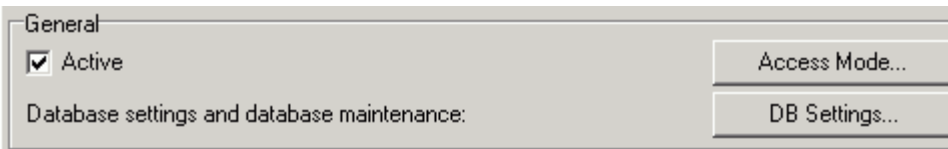
Spam classification scores are lowered. Spam score adjustment values are set higher than in other templates.

There are some features which are not automatically used by any of these templates and must be activated individually: AntiSpam Live, Greylisting, Spam reports, which will be discussed later.

Now let's go through the AntiSpam settings step by step.

General

The General settings area allows you to activate or deactivate AntiSpam and set an update schedule.

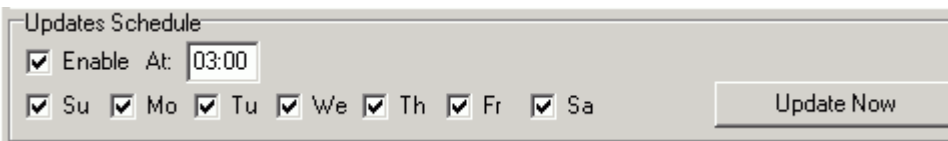


General

Active Access Mode...

Database settings and database maintenance: DB Settings...

Make sure **Active** is checked.



Updates Schedule

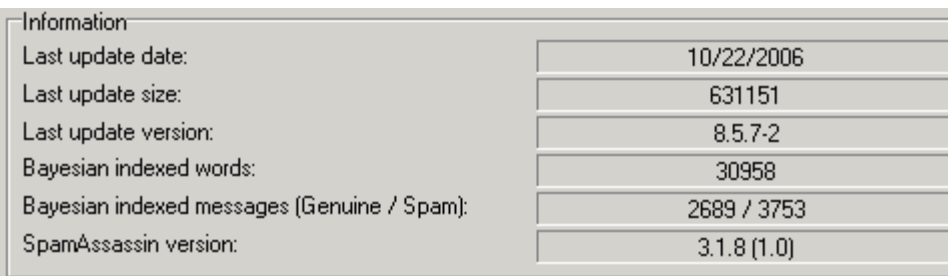
Enable At: 03:00 Update Now

Su Mo Tu We Th Fr Sa

Set an **Update Schedule** to make sure your AntiSpam is always up to date.

Enter a time for your update to happen.

Check the box for each day you want the update to happen.

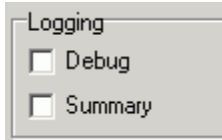


Information	
Last update date:	10/22/2006
Last update size:	631151
Last update version:	8.5.7-2
Bayesian indexed words:	30958
Bayesian indexed messages (Genuine / Spam):	2689 / 3753
SpamAssassin version:	3.1.8 (1.0)

Other

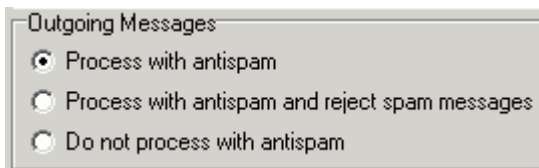
Settings related to the System, Outgoing messages and "Unknown Accounts"

Logging



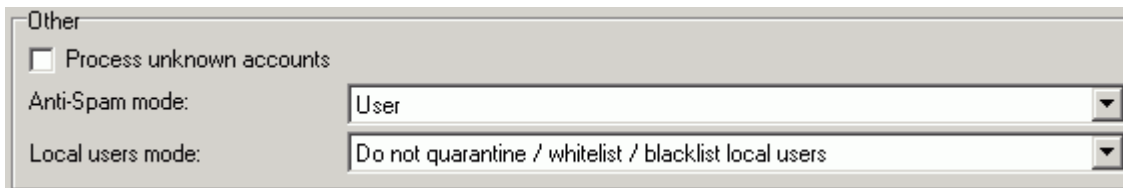
Check both boxes. Initially, while you are tuning your AntiSpam Settings, you are very likely to have messages that are incorrectly classified. Having full logging options allows you to investigate the reasons behind the incorrect classification and tweak your settings accordingly.

Outgoing Messages



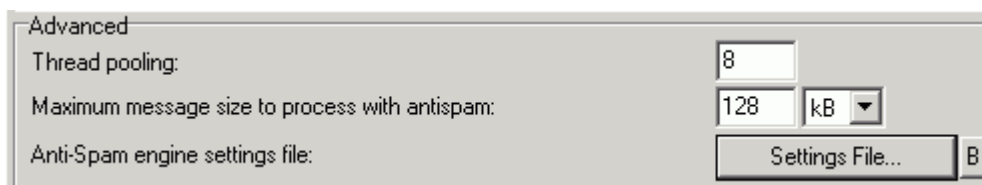
Your server can be blacklisted by the other servers when sending too many spam messages to them. Hence the recommended setting is **Process with AntiSpam**.

Other



This is for messages destined for an email address that does not exist on your server, but may be delivered to an account via some filter or rule. If you set "Reject mail" for unknown accounts in your domain basic settings, you do not need to check this option at all.

Advanced



Leave these at the standard installation defaults.

Action

This is where you set what happens to a message after all the heavy work is done and a Spam Score is assigned to the message

General

Setting	Checkbox	Slider	Value
Score required to quarantine message:	<input type="checkbox"/>	[Slider]	3.00
Score required to classify message as spam:	<input checked="" type="checkbox"/>	[Slider]	3.00
Score required to refuse message:	<input checked="" type="checkbox"/>	[Slider]	10.00

Score required to quarantine message is greyed out because we haven't yet enabled the quarantine engine, just ignore it for now.

Check **Score required to classify message as spam**. Set slider value to **3.00**.

Check **Score required to refuse message**. Set slider value to **10.00**.

Refusal

Refuse message action:	Reject
Archive refused messages to account:	[Empty field] ...

Set **Refuse message action** to **Reject**.

Spam

Spam

Add text to Subject of spam message: [Spam]

Place spam messages under spam folders

Integrate spam folder with IMAP (Folder name): Spam

Delete spam messages from spam folders when older than (Days): 30

Check **Add text to Subject of spam message**. Set text value to something like [Spam].

Enter a value for **Delete spam messages from spam folders when older than (Days)** to a suitable number of days- we recommend 30 initially.

Reports

The Reports tab allows you to have IceWarp Server send automated reports to your Users listing Quarantined and Spam messages that they should action. This is a great way of getting your Users to help setting up your system for you.

Reports

Enable quarantine reports Schedule...

Enable spam folder reports

Logging

Sender: <Spam Admin>

From: Spam Report <>

Report mode: All items

Engine URL: http://mail.domain.com:32000/challenge/

Run Now Run Now in Debug Mode

Check **Enable spam folder reports**.

Set **Sender** to something meaningful .

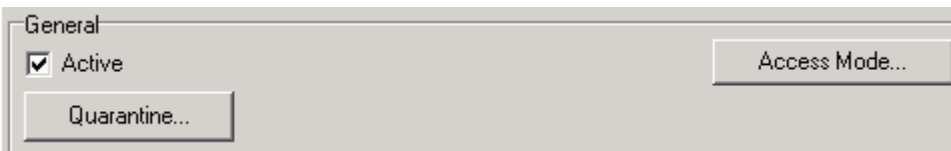
Enter the **From** header information you wish to appear in the reports.

Set **Report mode** to **New items**.

Quarantine

This is where we tell IceWarp Server how to handle messages that are to be quarantined. Remember, quarantined messages are held in a quarantine queue awaiting manual intervention by the intended recipient, an administrator, or the original sender.

General



The screenshot shows a window titled "General" with a tabbed interface. The "Active" checkbox is checked. There are two buttons: "Quarantine..." and "Access Mode...".

Check the **Active** box to use the quarantine function.

Options



The screenshot shows a window titled "Options" with a tabbed interface. It contains three settings: "Remove pending messages after (Days):" with a text box containing "21"; "Deliver expired messages to mailbox as spam" with a checked checkbox; and "Engine URL:" with a text box containing "http://mail.domain.com:32000/challenge/".

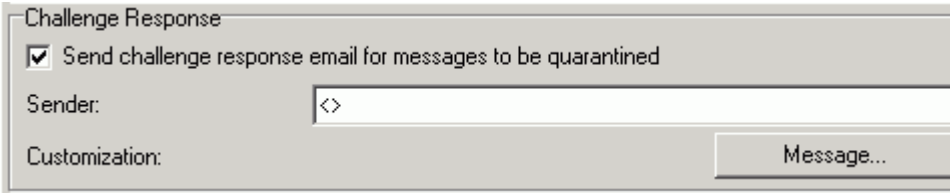
Enter a value in the box next to **Remove pending messages after (Days)**. If a message goes into Quarantine and is not manually actioned within this time it will be moved on - Recommended setting 21.

Check the box to **Deliver expired messages to mailbox as spam** - so after the 21 days in Quarantine the message will be marked as Spam and delivered to the User. If you do not check this option the message is permanently deleted and you run the risk of losing legitimate messages.

Select **Do not quarantine local users** from the **Local users mode** drop-down - this means that messages sent from one of your Users to another of your Users will not be Quarantined.

Modify the **Engine URL** to point to your domain - so if your domain is MyDomain.com, modify this field to `http://www.MyDomain.com/challenge` - this is used for the challenge Response system (see below)

Challenge Response



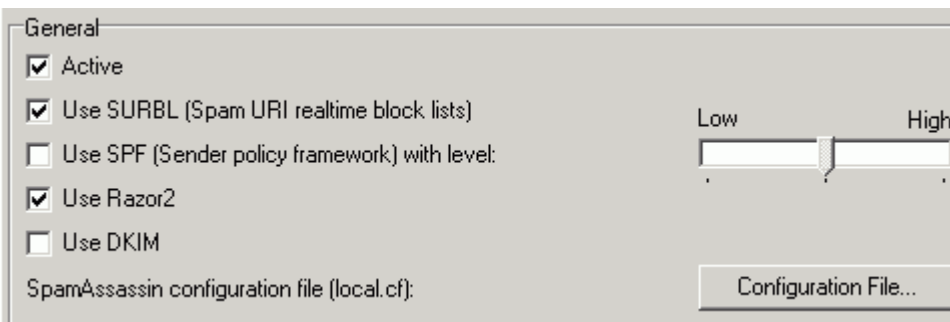
The screenshot shows a window titled "Challenge Response". It contains a checked checkbox labeled "Send challenge response email for messages to be quarantined". Below this is a "Sender:" label followed by a text input field containing "<>". At the bottom left is a "Customization:" label, and at the bottom right is a "Message..." button.

Check the box to **Send challenge response** emails - this will send an email to the sender of a quarantined message asking him to confirm he is human by visiting a web page and entering some information. This takes some effort away from your Users and Administrators.

SpamAssassin

SpamAssassin is a third-party AntiSpam technology that is incorporated within IceWarp Server. SpamAssassin itself incorporates a number of differently named technologies, each of which can be used in your fight against Spam.

General



The screenshot shows a window titled "General". It contains several checkboxes: "Active" (checked), "Use SURBL (Spam URI realtime block lists)" (checked), "Use SPF (Sender policy framework) with level:" (unchecked), "Use Razor2" (checked), and "Use DKIM" (unchecked). To the right of the "Use SPF" checkbox is a slider control with "Low" on the left and "High" on the right, with a vertical bar in the middle. At the bottom left is the text "SpamAssassin configuration file (local.cf):" and at the bottom right is a "Configuration File..." button.

Check the **Active** box - this switches on SpamAssassin processing. If this box is unchecked, all the other boxes will be greyed out and unusable.

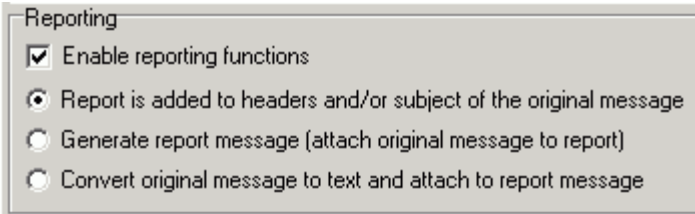
Check the box to **Use SURBL** – it checks the links found within a message to see if they are known to be Spammer target sites.

Do not check the box to **Use SPF** - SPF is not widely used as yet and can lead to many genuine messages being classified as Spam.

Check the box to **Use Razor2**.

Do not check the box to **Use DKIM** - DKIM is not widely in use as yet and can lead to many genuine messages being classified as Spam.

Reporting



The screenshot shows a window titled "Reporting" with the following options:

- Enable reporting functions
- Report is added to headers and/or subject of the original message
- Generate report message (attach original message to report)
- Convert original message to text and attach to report message

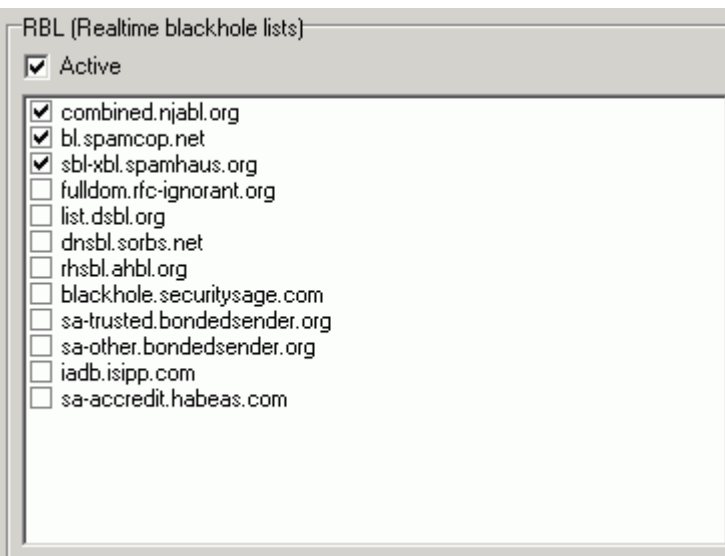
Check the **Enable reporting functions** box.

Select the **Report is added to headers** option.

RBL

RBL is a system whereby IceWarp Server can check whether a message has been sent from a known source of Spam.

You would probably have this option switched on in the Mail Service - Security Node, in which case you don't need to switch it on here as well. If you don't have this enabled in the Security Node then you should enable it here:



The screenshot shows a window titled "RBL (Realtime blackhole lists)" with the following options:

- Active
- combined.njabl.org
- bl.spamcop.net
- sbl-xbl.spamhaus.org
- fulldom.rfc-ignorant.org
- list.dsbl.org
- dnsbl.sorbs.net
- rhsbl.ahbl.org
- blackhole.securitysage.com
- sa-trusted.bondedsender.org
- sa-other.bondedsender.org
- iadb.isipp.com
- sa-accredit.habeas.com

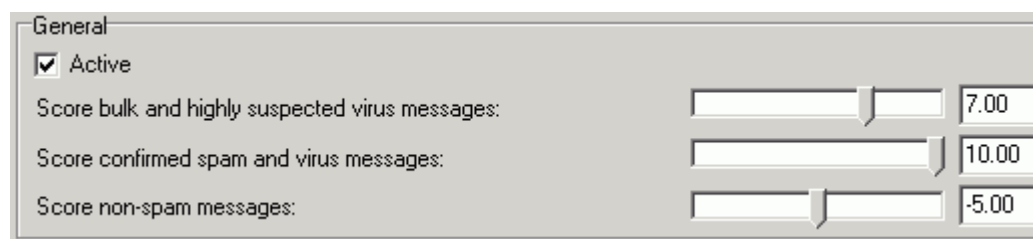
Check the **Active** box

Check the boxes for combined.jabl.org, bl.spamcop.net and sbl-xbl.spamhaus.org (recommended settings).

Anti-Spam Live

"Anti-Spam Live analyzes large volumes of Internet traffic in real time, and identifies new spam, virus and Phishing outbreaks based on their characteristic mass distribution patterns. Emerging outbreaks are identified moments after they are introduced into the Internet."

This can significantly help in identifying bulk and spam emails.



General

Active

Score bulk and highly suspected virus messages:

Score confirmed spam and virus messages:

Score non-spam messages:

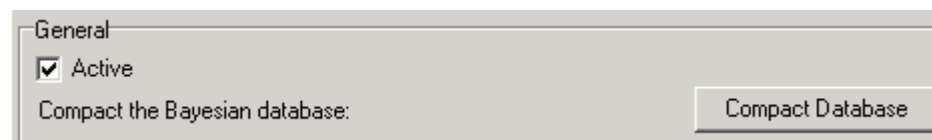
If you have an AntiSpam license then check **Active**.

Set **Score bulk to...** 7.00

Set **Score confirmed spam...** to 10.00

Bayesian Filters

When applied to Spam, it collects the frequency of spam messages and genuine messages, and the frequency of the words occurring in those messages. When a new message comes in, it check the words in the new message against the statistics in the database, and makes an "informed guess" as to whether the new message is Spam.



General

Active

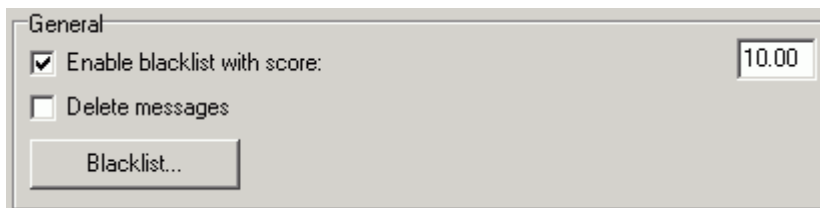
Compact the Bayesian database:

Just check the **Active** box.

Black & White List

Blacklist

General

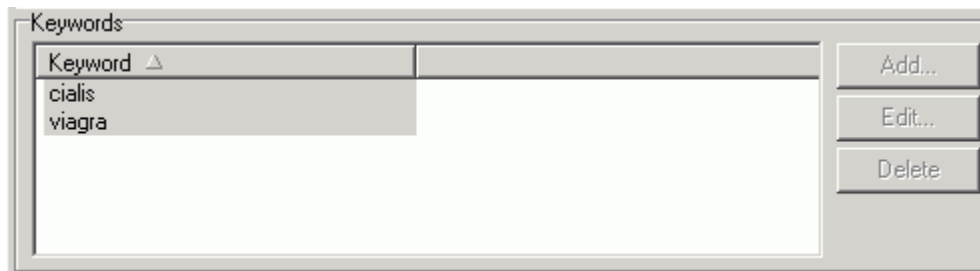


The screenshot shows a window titled 'General' with the following elements:

- A checked checkbox labeled 'Enable blacklist with score:' followed by a text input field containing '10.00'.
- An unchecked checkbox labeled 'Delete messages'.
- A button labeled 'Blacklist...'.

Check **Enable blacklist with score** to enable Blacklist processing to modify the spam score of a message. Enter a value to modify the score by.

Keywords



The screenshot shows a window titled 'Keywords' with the following elements:

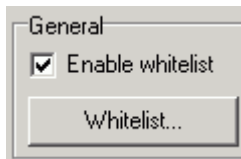
- A table with a header 'Keyword' and a small triangle icon. The table contains two rows: 'cialis' and 'viagra'.
- Three buttons on the right side: 'Add...', 'Edit...', and 'Delete'.

Add the keywords which if found within a message, will cause the message to have its spam score increased.

Whitelist

If an email address is put on the whitelist, IceWarp Server will simply pass it through unchecked.

General

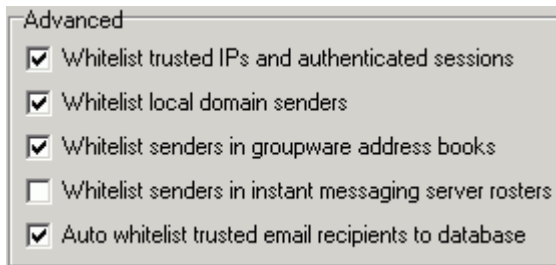


Check **Enable whitelist**.

Set **Whitelist mode** to **User** and addresses will be whitelisted for the User who whitelists it.

This setting is the most safe and hence is recommended.

Advanced



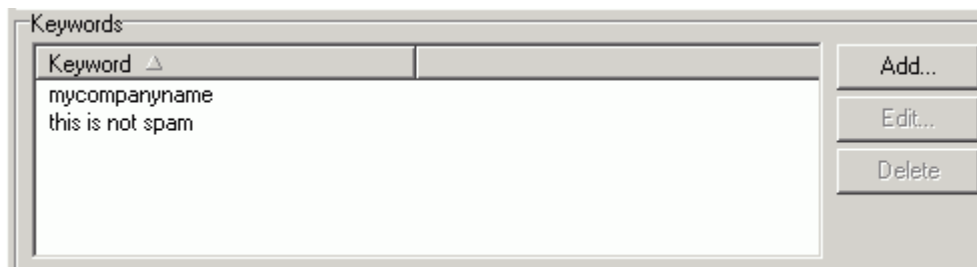
Check **Whitelist trusted IPs and authenticated sessions** which will add IP addresses in "trusted" lists and authenticated session items to the whitelist.

Check **Whitelist Local domain senders**.

Check **Whitelist senders in Groupware address books**.

Check **Auto whitelist trusted email addresses to database**. This option adds all trusted addresses added to the Whitelist Database.

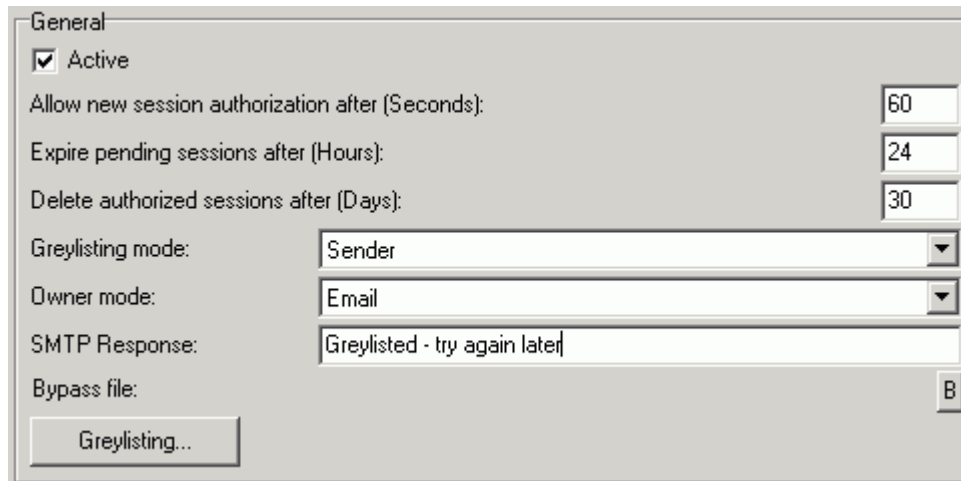
Keywords



Use the Keywords section to whitelist the messages with the specified words in text.

Greylisting

"Greylisting works on the fact that Spammers want to get their emails out at the speed of light. They can't be bothered waiting for servers, they just want to send their 14 million messages in the next two minutes or give up trying - so we let them give up!"



The screenshot shows the 'General' tab of a configuration window. It contains the following settings:

- Active
- Allow new session authorization after (Seconds): 60
- Expire pending sessions after (Hours): 24
- Delete authorized sessions after (Days): 30
- Greylisting mode: Sender
- Owner mode: Email
- SMTP Response: Greylisted - try again later
- Bypass file: B
- Greylisting... button

Check the **Active** box

Set the **Allow new session authorization** to **60**.

Set **Expire pending sessions** to **24**.

Set **Delete authorized sessions** to **30**.

Select **Sender** for the **Greylisting mode**.

Put something meaningful in the **SMTP Response**, such as "Greylisted - come back later" - so "real" administrators can see why their server could not get through.

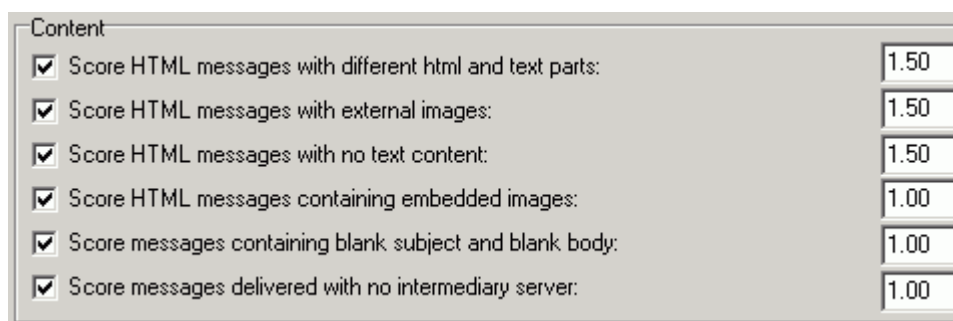
Learning Rules

Ignore this until your system is running nicely, until you are confident that messages are being processed correctly.

Miscellaneous

Content

A lot of the Spam "bombing" software that spammers use do not format messages correctly, i.e. according to the rules. IceWarp Server can take advantage of this in its fight against Spam.

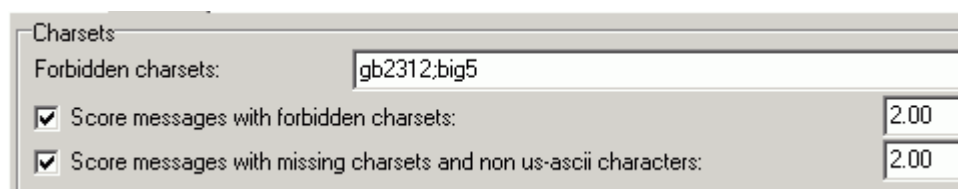


Option	Score
<input checked="" type="checkbox"/> Score HTML messages with different html and text parts:	1.50
<input checked="" type="checkbox"/> Score HTML messages with external images:	1.50
<input checked="" type="checkbox"/> Score HTML messages with no text content:	1.50
<input checked="" type="checkbox"/> Score HTML messages containing embedded images:	1.00
<input checked="" type="checkbox"/> Score messages containing blank subject and blank body:	1.00
<input checked="" type="checkbox"/> Score messages delivered with no intermediary server:	1.00

The setup is balanced, it is recommended to leave all the settings as they are.

Charset

Use this if it suits your user base and the character sets they use.



Option	Score
Forbidden charsets: <input type="text" value="gb2312;big5"/>	
<input checked="" type="checkbox"/> Score messages with forbidden charsets:	2.00
<input checked="" type="checkbox"/> Score messages with missing charsets and non us-ascii characters:	2.00

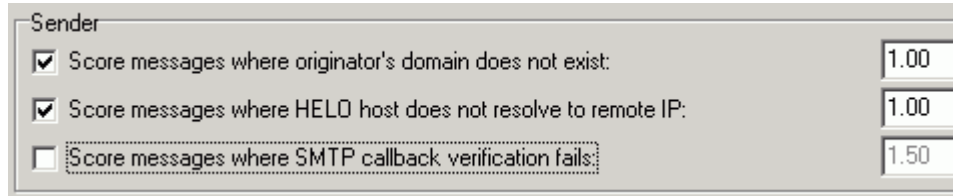
Specify any unwarranted character sets in **Forbidden charsets**.

Specify a list of charsets that you consider likely to be spam.

Set the spam score which will be added to the message with the specified charset to 2.00 and do the same with the Score messages with missing charsets and non us-ascii characters option.

Sender

The Sender section allows you to modify the Spam Score according to the sender information of the message.



Condition	Score
<input checked="" type="checkbox"/> Score messages where originator's domain does not exist:	1.00
<input checked="" type="checkbox"/> Score messages where HELO host does not resolve to remote IP:	1.00
<input type="checkbox"/> Score messages where SMTP callback verification fails:	1.50

Set **Score messages where sender's domain does not exist** and **Score messages where HELO host does not resolve to remote IP** to **1.00**.

Index

A

Action • 7
Advanced • 6, 14
Anti-Spam Live • 12
AntiSpam Templates • 4

B

Bayesian Filters • 12
Black & White List • 13
Blacklist • 13

C

Challenge Response • 10
Charset • 16
Content • 16

G

General • 5, 7, 9, 10, 13, 14
Greylisting • 15

H

How it works • 3

I

IceWarp Server AntiSpam Quick Start • 3
Introduction • 3

K

Keywords • 13, 14

L

Learning Rules • 15

Logging • 6

M

Miscellaneous • 16

O

Options • 9
Other • 5, 6
Outgoing Messages • 6

Q

Quarantine • 9

R

RBL • 11
Refusal • 7
Reporting • 11
Reports • 8

S

Sender • 17
Spam • 8
SpamAssassin • 10

W

Whitelist • 13